

R D @

Recht Digital

Geschäftsführende

Herausgeber:

Prof. Dr. Florian Möslein
Prof. Dr. Thomas Riehm
Dr. Markus Kaulartz

Herausgegeben von:

Tom Braegelmann
Dr. Julia von Buttler
Prof. Dr. Martin Ebers
Dr. Tobias Faber
PD Dr. Martin Fries
Dr. Dennis-Kenji Kipker
Nico Kuhlmann
Dr. Christina-Maria Leeb
Prof. Dr. Kai von Lewinski
Robin Matzke
Dr. Henning Müller
Prof. Dr. Sebastian Omlor
Dr. Gerald Reger
Dr. Frank Remmert
Dr. Thomas Sassenberg
Prof. Dr. Martin Schmidt-Kessel
Dr. Lea Maria Siering
Dr. Alexander Steinbrecher
Prof. Dr. Björn Steinrötter
Rebekka Weiß
Benedikt Windau
Prof. Dr. Thomas Wischmeyer

Schriftleiter:

Christopher Rennig

AUFSÄTZE

Digitale Finanzdienstleistungen

Sebastian Omlor/Aurelia Birne: Digitales Zentralbankgeld im Euroraum 1

Thorsten Voß: Lessons to be learned? – Zur causa Wirecard und der aufsichtsrechtlichen Regulierung von FinTechs 11

Künstliche Intelligenz

Simon Apell/Markus Kaulartz: Rechtlicher Schutz von Machine Learning-Modellen 24

Florian Möslein: Die normative Kraft des Ethischen – Ein Fallbeispiel zur Effektivität von Leitlinien für Künstliche Intelligenz 34

Thomas Riehm: Nein zur ePerson! – Gegen die Anerkennung einer digitalen Rechtspersönlichkeit 42

E-Justice/E-Government

Martin Fries/Rupprecht Podszun/Benedikt Windau: Virtuelle Verhandlung statt fliegendem Gerichtsstand – Fairer Wettbewerb durch technischen Fortschritt 49

RECHTSPRECHUNG

Digitale Rechtsdienstleistungen

OLG Köln: Rechtmäßigkeit des Verwendung von Textbausteinen in einer Berufungsbegründung (*Frank Remmert*) 56

OLG Köln: Online-Dokumentengenerator keine erlaubnispflichtige Rechtsdienstleistung i.S.d. RDG (*Christina-Maria Leeb*) 57

E-Justice/E-Government

LG Mannheim: Anforderungen an die Bearbeitbarkeit eines elektronischen Dokuments gem. § 130a II ZPO (*Henning Müller*) 59

OLG Hamm: Grundsatz des fairen Verfahrens – nicht gespeicherte Messdaten (*Thomas Wischmeyer/Oskar Schumacher*) 61

LAG Düsseldorf: Zur Anfechtbarkeit der Ablehnung einer Videokonferenz-verhandlung (*Benedikt Windau*) 63



Blockchain, Krypto & Co.

VORTEILE AUF EINEN BLICK

- › wissenschaftliche Aufarbeitung
- › umfassende Darstellung der rechtlichen Einordnung und Regulierung von Kryptowährungen und Initial Coin Offerings
- › hoher Praxisbezug

Die Blockchain-Technologie,

Kryptowährungen, und ICOs bieten neue Möglichkeiten der Bezahlung, der Kapitalbeschaffung und des Investments. Die praktische Bedeutung ist schon jetzt enorm. Gleichzeitig sind grundlegende rechtliche Fragen zum Teil noch unbeantwortet. Das neue Handbuch beleuchtet die **Rechtsfragen** aus allen Blickwinkeln und gibt **Hilfestellung** für praxisgerechte **Rechtslösungen**.

Aus dem Inhalt

- › Technische und wirtschaftliche Grundlagen
- › Einführung in die Technologie, Token-Arten, Begriffsbestimmungen
- › Kryptotoken im Rechtsverkehr
- › Anwendbares Recht und internationale Zuständigkeit, Rechtsnatur und Übertragung von Token, Verträge über Token, Kryptowährungen als Zahlungsmittel, Mining-pools, Verbraucherschutz
- › Kapitalmarkt- und Bankenrecht
- › Wertpapierbegriff und rechtliche Anforderungen an Initial Coin Offerings (ICOs), Finanzintermediäre und Kryptobörsen, Marktmissbrauchsrecht
- › Compliance und Datenschutz
- › Geldwäscheprävention, Anonymität, Datenschutz
- › Steuern und Bilanzierung
- › Ertragssteuern, Umsatzsteuer, Bilanzierung
- › Strafrecht
- › Phänomenologie, internationales Strafrecht, Kern- und Nebenstrafrecht, Strafverfahren



Maume/Maute

Rechtshandbuch Kryptowerte

2020. XXII, 626 Seiten.

In Leinen € 149,-

ISBN 978-3-406-73433-5

☰ beck-shop.de/26353222

Georg Eisenreich

Digitalisierung und Recht

Bill Gates hat es auf den Punkt gebracht. Er sagte: „Wir überschätzen immer den Wandel, der in den nächsten zwei Jahren passieren wird und unterschätzen den Wandel, der in den nächsten zehn Jahren passieren wird.“ Er hat Recht. Deshalb muss Deutschland bei der Digitalisierung Tempo machen. Dabei führen der rasante technologische Fortschritt und dynamische Entwicklungen in Wirtschaft und Gesellschaft zu neuen rechtlichen, politischen und ethischen Fragen. Diese müssen diskutiert und geklärt werden, zum Beispiel: Wer haftet nach welchem Maßstab bei Unfällen mit autonom fahrenden Autos? Wie können Meinungsfreiheit und Ehrschutz in Zeiten von Hass und Hetze in den sozialen Medien in ein ausgewogenes Verhältnis gebracht werden? Wie kann Europa seine digitale Souveränität zurückgewinnen? Wie kann die Markt- und Datenmacht monopolartiger Internetkonzerne so begrenzt werden, dass sie keine Gefahr für die Demokratie und den freien Wettbewerb darstellen?



Viele Menschen nutzen die Vorteile der Digitalisierung. Sie erwarten von Staat und Wirtschaft in immer mehr Bereichen schnelle, bequeme, kostengünstige digitale Lösungen. Digitale Dienstleistungen werden daher in den nächsten Jahren sowohl den Alltag als auch den Markt weiter verändern. Dies gilt für Finanzdienstleistungen und Verwaltungsleistungen genauso wie für den Zugang zum Recht und die Rechtsdurchsetzung. Wer hat es etwa vor zehn Jahren auf sich genommen, eine Entschädigung für Flugverspätungen geltend zu machen? Inzwischen ist es ein digitales Massengeschäft von Legal Tech-Unternehmen. Für Legal Tech muss ebenso wie beispielsweise für FinTech oder InsurTech der Rechtsrahmen geklärt werden: Was sind die Möglichkeiten und Grenzen? Was wollen wir zulassen, was nicht? Notwendig sind Wertentscheidungen des Gesetzgebers.

Auch die Rechtspflege steht vor Veränderungen: Elektronischer Rechtsverkehr und E-Akte sind bereits Realität oder zumindest auf dem Weg. Die Veränderungen werden aber wesentlich tiefgreifender sein. Robo-Anwälte, die ihre KI-erzeugten Schriftsätze einem Richterautomat vorlegen, der algorithmenbasiert entscheidet – Traum oder Alptraum? Richterinnen und Richter, Rechtsanwältinnen und Rechtsanwälte wird es immer geben und muss es nach meiner Überzeugung immer geben. In der Zukunft werden sich jedoch gerichtliche Verfahren, insbesondere im Zivilrecht, von den heutigen Abläufen deutlich unterscheiden. Innovative Vorschläge hierzu hat die von den Präsidentinnen und Präsidenten der Oberlandesgerichte, des Kammergerichts, des Bayerischen Obersten Landesgerichts und des Bundesgerichtshofs eingesetzte Arbeitsgruppe „Modernisierung des Zivilprozesses“ zur Diskussion gestellt.

Bei der Digitalisierung geht es um alles: Unseren Wohlstand, unsere Werte, unsere Demokratie. Die Themen werden daher nicht ausgehen. „Recht Digital“ bietet ein Forum, um sie zu diskutieren.

Georg Eisenreich, MdL, ist Bayerischer Staatsminister der Justiz

Das umfassende Kompendium zur FinTech-Branche.

Die Schwerpunkte

- › Zahlungsverkehr (Payments)
- › Beteiligungsfinanzierung (Crowdfunding, Crowdfunding)
- › Kreditfinanzierung (Crowdlending)
- › Effektengeschäft
- › Vermögensanlage (Robo Advice)
- › Versicherung (InsurTech)
- › Geld/Zahlungsmittel
- › Blockchain

Das neue Werk

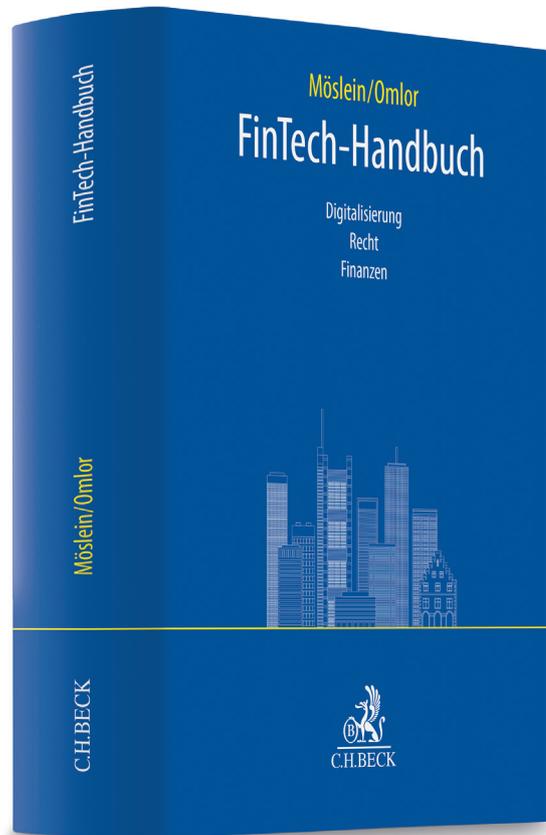
stellt die FinTech-Branche erstmals in ihrer gesamten Breite dar. Das Handbuch behandelt die dogmatischen Grundlagenfragen ebenso wie die forensische Anwendungspraxis, die technischen Funktionsweisen und die ökonomische Rahmenbedingungen. Zivil- und Aufsichtsrecht finden ebenso Berücksichtigung wie die ökonomischen und internationalen Bezüge.

Herausgeber

Prof. Dr. Florian **Möslein**, Dipl.-Kfm., LL.M., und Prof. Dr. Sebastian **Omlor**, LL.M., LL.M. Eur., Ko-Direktoren des Instituts für das Recht der Digitalisierung an der Philipps-Universität Marburg sowie das hochkarätige Autorenteam sind führende Experten in den einzelnen Bereichen.

Bestens geeignet

für Rechtsanwälte im Finanz-, Bank-, Kapitalmarkt-, Versicherungs- und IT-Recht sowie für FinTech-Inhouse-Juristen und Unternehmensberater.



Möslein/Omlor FinTech-Handbuch

2019. XXVI, 655 Seiten
In Leinen € 179,-
ISBN 978-3-406-71366-8

☰ beck-shop.de/20360107

Inhalt

MAGAZIN

Editorial: Digitalisierung und Recht (<i>Georg Eisenreich</i>)	3
Magazin: Gesetzgebung, Nachrichten, Europa, Sonstiges, Heftvorschau (<i>Redaktion</i>)	6
Interview: Datenschutz ist Standortvorteil (<i>Stefan Brink</i>)	8
Tech & Tools: Automatisierung von Expertenwissen	9

AUFSÄTZE

Digitale Finanzdienstleistungen	
<i>Sebastian Omlor/Aurelia Birne</i> , Digitales Zentralbankgeld im Euroraum	1
<i>Thorsten Voß</i> , Lessons to be learned? – Zur causa Wirecard und der aufsichtsrechtlichen Regulierung von FinTechs	11
Künstliche Intelligenz	
<i>Simon Apel/Markus Kaulartz</i> , Rechtlicher Schutz von Machine Learning-Modellen	24
<i>Florian Möslein</i> , Die normative Kraft des Ethischen – Ein Fallbeispiel zur Effektivität von Leitlinien für Künstliche Intelligenz	34
<i>Thomas Riehm</i> , Nein zur ePerson! – Gegen die Anerkennung einer digitalen Rechtspersönlichkeit	42
E-Justice/E-Government	
<i>Martin Fries/Rupprecht Podszun/Benedikt Windau</i> , Virtuelle Verhandlung statt fliegendem Gerichtsstand – Fairer Wettbewerb durch technischen Fortschritt	49

RECHTSPRECHUNG

Digitale Rechtsdienstleistungen	
<i>OLG Köln, Beschluss vom 18.8.2020 – 15 U 171/19</i> , Rechtmäßigkeit des Verwendung von Textbausteinen in einer Berufungsbegründung (<i>Frank Remmert</i>)	56
<i>OLG Köln, Urteil vom 19.6.2020 – 6 U 263/19</i> , Online-Dokumentengenerator keine erlaubnispflichtige Rechtsdienstleistung i.S.d. RDG (<i>Christina-Maria Leeb</i>)	57
E-Justice/E-Government	
<i>LG Mannheim, Urteil vom 4.9.2020 – 1 S 29/20</i> , Anforderungen an die Bearbeitbarkeit eines elektronischen Dokuments gem. § 130 a II ZPO (<i>Henning Müller</i>)	59
<i>OLG Hamm (3. Senat für Bußgeldsachen), Beschluss vom 25.11.2019 – 3 RBs 307/19</i> , Grundsatz des fairen Verfahrens – nicht gespeicherte Messdaten (<i>Thomas Wischmeyer/Oskar Schumacher</i>)	61
<i>LAG Düsseldorf, Beschluss vom 2.7.2020 – 4 Ta 200/20</i> , Zur Anfechtbarkeit der Ablehnung einer Video-konferenzverhandlung (<i>Benedikt Windau</i>)	63

GESETZGEBUNG

Schuldrecht für digitale Produkte

Das Bundesministerium der Justiz und für Verbraucherschutz (BMJV) hat einen Gesetzentwurf veröffentlicht, mit dem das Schuldrecht bei Verbraucherverträgen über digitale Produkte erstmals speziell geregelt werden soll. Kernstücke der Neuregelung, mit der die sogenannte Digitale-Inhalte-Richtlinie (2019/770) umgesetzt werden soll, sind ein komplettes Mängelgewährleistungsregime für Software/Apps und andere digitale Inhalte sowie für zwei Formen digitaler Dienstleistungen. Die Regeln sollen auch gelten, wenn etwa bei sozialen Netzwerken nicht mit Geld, sondern mit personenbezogenen Daten bezahlt wird.

Der „Entwurf eines Gesetzes zur Umsetzung der Richtlinie über bestimmte vertragsrechtliche Aspekte der Bereitstellung digitaler Inhalte und digitaler Dienstleistungen“ sieht für sämtliche Verbraucherverträge über digitale Inhalte (etwa Musik- und Videodateien, Software/Apps, E-Books) ein eigenes Gewährleistungsrecht bei Sach- und Rechtsmängeln vor. „Dabei geht er von einem eigenen, objektiven Sachmangelbegriff aus, von dem man nur sehr schwer abweichen kann“, erläutert Prof. Dr. Martin Schmidt-Kessel, Inhaber eines Lehrstuhls für Deutsches und Europäisches Verbraucherrecht an der Universität Bayreuth und Mitherausgeber dieser Zeitschrift. Als Gewährleistungsrechte sieht der Entwurf den Anspruch auf Nacherfüllung, auf Minderung, das Recht zur Beendigung des Vertrags und einen Anspruch auf Schadens-/Aufwendungsersatz vor. „Es gibt zwar eine neue Form der Vertragsbeendigung, aber ansonsten sind die Instrumente nicht neu“, so Schmidt-Kessel.

Das Gewährleistungsregime gilt auch, wenn digitale Inhalte auf körperlichen Datenträgern gespeichert sind (z.B. auf CDs, DVDs) und bei Hybridprodukten (wie Spielen). Außerdem sind zwei Formen digitaler Dienstleistungen umfasst, nämlich Cloud-Anwendungen und soziale Netzwerke. Dabei stehen den Verbrauchern die Gewährleistungsrechte auch dann zu, wenn sie mit personenbezogenen Daten bezahlen – für Schmidt-Kessel einer der Kernpunkte des vorgelegten Referentenentwurfs, den er für „ziemlich gut gelungen“ hält. Da er „in weiten Teilen eine echte 1:1-Umsetzung“ sei, werde der Entwurf „in der Substanz wohl so durchgehen“.

Das BMJV hat auch noch den „Entwurf eines Gesetzes zur Änderung des Bürgerlichen Gesetzbuchs und des Einführungsgesetzes zum Bürgerlichen Gesetzbuche in Umsetzung der EU-Richtlinie zur besseren Durchsetzung und Modernisierung der Verbraucherschutzvorschriften der Union“ vorgelegt. Hier sollen Verbraucher unter anderem von Transparenzpflichten für Online-Marktplätze wie Amazon oder eBay und Informationspflichten beim Weiterverkauf von Eintrittskarten über Ticketbörsen profitieren.

Kritik an Personenkennziffer

Die Bundesregierung plant eine Registermodernisierung, um Inkonsistenzen und Mehrfacheingaben von Daten zu vermeiden. Der Gesetzentwurf für ein Registermodernisierungsgesetz (RegMoG) sieht dazu eine registerübergreifende Verknüpfung aller sogenannten Basisdaten natürlicher Personen mittels Schaffung einer einheitlichen Identifikationsnummer vor. Hierfür soll das Identifikationsnummerngesetz (IDNrG) beschlossen werden, welches auf die vorhandenen Strukturen der Steuer-ID zurückgreift.

Während die Zielsetzung des Vorhabens weitgehend Unterstützung erfährt, gibt es an der Umsetzung viel Kritik. Es gibt datenschutzrechtliche und verfassungsrechtliche Bedenken. Prof. Dr. Kai von Lewinski von der Universität Passau, Mitherausgeber dieser Zeitschrift, bringt das in einem Interview mit der NJW wie folgt auf den Punkt: „Die Identifikationsnummer rührt an der Urangst vor einer ‚Vollverdattung‘. Zwar sind Personenkennzeichen als solche persönlichkeitsrechtlich ziemlich trivial; sie sind aber der Schlüssel zu gehaltvollen Informationen über eine Person. Und nicht nur irgendein Schlüssel, sondern der Generalschlüssel. Anhand von Personenkennziffern können umfassende Persönlichkeitsprofile erstellt werden.“ Letzteres sei nach der bisherigen verfassungsgerichtlichen Rechtsprechung gesperrt.

Die Gesellschaft für Informatik (GI) weist darauf hin, dass die Umsetzung im jetzigen Gesetzentwurf auch nicht dem aktuellen Stand der Technik entspreche. Dieser ermögliche datenschutzfreundlichere Lösungen, wie sie etwa in Österreich eingesetzt würden, so Prof. Dr.-Ing. Christoph Sorge, Inhaber des Lehrstuhls für Rechtsinformatik an der Universität Saarbrücken und Experte des Fachbereichs „Informatik in Recht und Öffentlicher Verwaltung“ der GI.

NACHRICHTEN

Kritik an Stand der Digitalisierung

Der Nationale Normenkontrollrat (NKR) hat seinen Jahresbericht 2020 vorgelegt. Er trägt den Titel: „Krise als Weckruf: Verwaltung modernisieren, Digitalisierungsschub nutzen, Gesetze praxistauglich machen“ In Kapitel 2, das sich der Digitalisierung in der Rechtsetzung und der Verwaltung widmet, kritisiert das Kontrollgremium den aktuellen Entwicklungsstand. Obwohl seit Jahren über digitale Verwaltungsdienstleistungen, intelligent vernetzte Behörden-Register und digitaltaugliche Gesetze geredet werde, hätten Bund und Länder diese Hausaufgaben nicht gemacht. Der NKR mahnt insbesondere eine zügige und transparente Umsetzung des Onlinezugangsgesetzes (OZG) und eine Registermodernisierung an. Eine weitere Forderung des Rates: Gesetze müssten digitaltauglich werden.

„Die Digitalisierung fängt beim Gesetzentwurf an. Wir müssen die Vollzugs- und Digitaltauglichkeit unserer Gesetze verbessern und mit einem Digital-TÜV systematisch kontrollieren“, heißt es dazu im Bericht. Grundsätzlich solle jedoch ein pragmatischer Ansatz verfolgt werden: „Lieber ohne gesetzliche Anpassungen auskommen, dafür aber zügiger digitalisieren.“ Der vollständige Bericht ist auf der Webseite des Normenkontrollrats abrufbar.

EUROPA

Haftung beim Einsatz von KI

Das EU-Parlament hat eine Entschlieung zur „Regelung der zivilrechtlichen Haftung beim Einsatz K nstlicher Intelligenz“ verabschiedet. Eine vollst ndige  berarbeitung der bisher gut funktionierenden Haftungsvorschriften ist nach Auffassung des Parlaments nicht erforderlich. Stattdessen fordern die Abgeordneten, dass k nftig neben dem Hersteller eines Produkts mit risikoreicher KI auch der Betreiber haften muss. Dabei soll zwischen Hochrisiko- und allen anderen KI-Systemen unterschieden werden. Auerdem wird f r KI-Anwendungen mit hohem Risiko eine Versicherungspflicht f r deren Betreiber gefordert.

Regulierung von Krypto-Werten

Mit dem Vorschlag f r eine „Markets-in-Crypto-Assets-Verordnung“ hat die EU-Kommission im September einen einheitlichen Gesetzesrahmen f r Krypto-Werte vorgelegt. Darin werden die digitalen Wahrungen umfassend reguliert. So sollen Betreiber, die in einem Mitgliedstaat zugelassen sind, ihre Dienste in der ganzen EU erbringen d rfen. Als Sicherheitsvorkehrungen sind Eigenkapitalanforderungen, die Verwahrung von Vermogenswerten und Rechte der Anleger gegen ber den Emittenten vorgesehen; auerdem soll Anlegern ein Beschwerdeverfahren offen stehen. Emittenten von Stable Coins sollen strengeren Anforderungen unterliegen. Die EU-Kommission will mit der Verordnung Innovationen f rdern, zugleich aber auch die Finanzstabilitat wahren und Anleger vor Risiken sch tzen. Die Verordnung ist Teil eines Pakets zur Digitalisierung des Finanzsektors. Der Vorschlag muss noch vom Europaischen Parlament und Rat genehmigt werden. Dann k nnte er voraussichtlich Ende 2022 in Kraft treten und ware ohne Umsetzung in nationales Recht unmittelbar anwendbar.

Digitalisierung der Justiz

Der Rat der EU hat Schlussfolgerungen zur Nutzung der Chancen der Digitalisierung der Justiz angenommen. Darin fordert er die Kommission auf, bis Ende dieses Jahres

eine umfassende EU-Strategie f r die Digitalisierung der Justiz auszuarbeiten, mit der der Zugang zum Recht im gesamten Gemeinschaftsgebiet erleichtert und verbessert werden kann. Allerdings d rfte der Einsatz digitaler Technologien nicht die Grundsatze der Justizsysteme untergraben, namentlich die Unabhangigkeit und Unparteilichkeit der Gerichte, die Garantie eines wirksamen Rechtsschutzes und das Rechts auf ein faires und  ffentliches Verfahren. Der Rat fordert  berdies die F rderung digitaler Kompetenzen im Justizsektor. Angeh rige der Rechtsberufe m ssten digitale Instrumente wirksam nutzen k nnen. Zum m glichen Einsatz von KI im Bereich der Justiz wird betont, dass diese nicht die richterliche Unabhangigkeit oder das Recht auf ein faires Verfahren verletzen darf.

SONSTIGES

Neuerscheinungen



In dieser Rubrik wird auf interessante Neuerscheinungen aus dem Bereich Recht & Digitalisierung hingewiesen. Der Schwerpunkt wird auf der einschlagigen Praktikerliteratur liegen. Weil aber mit der wachsenden Bedeutung dieses Bereichs auch die Zahl der einschlagigen Reihen und Monographien stark zunimmt, werden in diesem Heft vier aktuelle Dissertationen erwahnt, die nicht nur f r Liebhaber der Materie von Interesse sind.

- Daniel Timmermann** • Legal Tech-Anwendungen • Diss. HU Berlin • Nomos 2020 • ISBN 978-3-8487-7773-0
- Christoph Rollberg** • Algorithmen in der Justiz • Diss. Potsdam • Nomos 2020 • ISBN 978-3-8487-6907-0
- David Saive** • Das elektronische Konnossement • Diss. Oldenburg • Mohr Siebeck 2020 • ISBN 978-3-16-159688-9
- Peter Scherer** • Blockchain im Wertpapierbereich • Mohr Siebeck 2020 • ISBN 978-3-16-158926-3

HEFTVORSCHAU 1 | 2021

J. Meier,  bertragung elektronischer Wertpapiere
M. Kramme, Der Gesetzentwurf zur Umsetzung der Digitale-Inhalte-Richtlinie
F. M slein/R. Zicari, Zertifizierung K nstlicher Intelligenz
J. Schmittmann, Virtuelle Glubigerversammlung



Datenschutz ist Standortvorteil

Die Datenschutzerfordernungen werden nach einer aktuellen Bitkom-Umfrage von der Wirtschaft als zusätzliche Belastung in der Corona-Krise empfunden, auch weil die Vorgaben teilweise unklar sind. Dazu hat maßgeblich das Urteil des EuGH zum sogenannten Privacy Shield (Schrems II) beigetragen, nach dem es für transatlantische Datentransfers keine gültige Rechtsgrundlage mehr gibt. Hierzu Fragen an Dr. Stefan Brink, den Datenschutzbeauftragten von Baden-Württemberg.

RD: Ist ein datenschutzkonformes Verhalten für Unternehmen derzeit faktisch unmöglich?

Brink: Keineswegs.

RD: Aber man kommt doch kaum noch ohne Software von US-Anbietern aus, die nach ihrem Heimatrecht verpflichtet sind, den Sicherheitsbehörden Datenzugriff zu ermöglichen. Ist die Nutzung solcher Programme nach Schrems II nicht per se unzulässig?

Brink: In vielen Bereichen gibt es Alternativen zu US-Anbietern – und auch diese bemühen sich, Angebote ohne Datentransfers in die USA bereitzustellen. Wer genau hinsieht, findet auch andere Lösungsansätze: In manchen Bereichen hilft eine anbieterunabhängige Verschlüsselung weiter – selbst Microsoft hatte zuletzt ein Joint Venture mit der Telekom im Angebot, welches die übergriffigen US-Behörden faktisch aussperrte. Aber sicher ist auch: Ohne intensive Bemühungen verlieren die US-Anbieter den europäischen Markt – und dieser Markt hat viel zu wenige nutzbare Alternativen.

RD: Die Datenschutzbeauftragten sind uneins, ob Microsoft Office 365 datenschutzgerecht eingesetzt werden kann. Sie bejahen das, die Mehrheit Ihrer Kollegen ist anderer Meinung. Was gilt denn jetzt?

Brink: Wir stimmen völlig darin überein, dass es bei Microsoft Office 365 dringender Verbesserungen bedarf. Umstritten ist der Weg hin zu einer Lösung – und da setzen einige Datenschützer nicht nur auf Druck, sondern auch auf Fairness im Umgang.

RD: Die Realität ist doch so: Ohne Microsoft würde das Land vermutlich zusammenbrechen – auch viele Behörden nutzen die Programme.

Brink: In der Tat haben wir es in vielen Bereichen mit einer ungesunden Angebotslage zu tun, Europa ist derzeit viel zu abhängig von US-Produkten. Wenn wir zukünftig in der Lage sein wollen, unsere hohen Rechts- und Datenschutzstandards auch praktisch umsetzen zu können, dann müssen wir für eine Verbreiterung der Angebote sorgen. Und

chinesische Anbieter sind hier sicher noch eine schlechtere Lösung – denn wenn es um unsere Werte geht, trennen uns von China Welten.

RD: Was empfehlen Sie Unternehmen, wie sie sich derzeit verhalten sollten?

Brink: Sie sollten aufmerksam die Entwicklung auf europäischer Ebene verfolgen, ihre Abhängigkeit von US-Anbietern prüfen und sie dort, wo möglich, zurückfahren. Sie sollten das Recht, insbesondere die DS-GVO, als das verstehen, was es ist: Ein Standortvorteil, der Europa einen nachhaltigen, fairen und demokratischen Weg ins digitale Zeitalter weist. Ohne wirtschaftliche Ausbeutung der Ressourcen persönlicher Daten, ohne Erpressbarkeit durch Anbieter und Regime, die unsere Werte nicht teilen.

RD: Die Wirtschaft empfindet den Datenschutz in der Corona-Krise als zusätzliche Belastung. Könnte man zur Abmilderung der Pandemie-Folgen wie in anderen Bereichen bestimmte Anforderungen befristet aussetzen oder beschränken?

Brink: Nein, denn das wäre töricht. Richtig verstandener und umgesetzter Datenschutz ist keine Gängelung, auch nicht in der Gesundheitskrise. Er schützt unser aller Rechte im digitalen Zeitalter – auch wenn unsere Sicherheit derzeit fragil ist, sollten wir unsere Freiheiten bewahren und nicht vorschnell aufgeben.

RD: Unabhängig davon muss doch aber der aktuell unklare Rechtszustand auch aus Sicht eines Datenschützers unbefriedigend sein. Wie würde es besser?

Brink: Der aktuelle Rechtszustand ist herausfordernd, aber es lohnt sich absolut, nach besseren Lösungen zu suchen. Ich verweise insofern auf die Orientierungshilfe meiner Behörde, die auf deren Webseite abrufbar ist. Wie es besser würde: Indem wir außereuropäischen Anbietern klare Vorgaben machen, wie wir uns freie und faire Datenverarbeitung vorstellen. Und der Versuchung widerstehen, uns angesichts US-amerikanischer Bedenkenlosigkeit und chinesischer Skrupellosigkeit zu abhängigen Konsumenten degradieren zu lassen.

AUFSÄTZE DIGITALE FINANZDIENSTLEISTUNGEN

Prof. Dr. Sebastian Omlor/Aurelia Birne*

Digitales Zentralbankgeld im Euroraum

Im Innovationsfeld zwischen Distributed Ledger Technology (DLT), Smart Contracts, Internet of Things (IoT), Industrie 4.0 und der Digitalisierung des Zahlungsverkehrs übernimmt seit einiger Zeit das digitale Zentralbankgeld immer mehr eine Protagonistenrolle. Nach einigem Zögern treten EZB und Bundesbank nunmehr verstärkt mit öffentlichen Stellungnahmen in Erscheinung. Daher soll nachfolgend der Rechtsrahmen eines solchen Projekts mit einem Fokus auf dem Geld-, Währungs- und Zahlungsdienstrecht beleuchtet werden.

I. Zahlungsverkehr im Zeitalter der Digitalisierung

[1] Die jüngste Herbsttagung 2020 der Deutschen Bundesbank zum Oberthema „Banking and Payments in the Digital World“ stand ganz im Zeichen der Digitalisierung des Zahlungsverkehrs. Das Tagungsprogramm fokussierte dabei besonders die Einführung von digitalem Zentralbankgeld (*Central Bank Digital Currency*, CBDC). In ihrer Rede stellte EZB-Präsidentin *Christine Lagarde* zwar heraus, eine finale Entscheidung über eine Einführung sei noch nicht gefallen. Zentral war jedoch die eindringliche Botschaft, der Euroraum könnte sich damit global eine technologische Führungsposition sichern: „Introducing a digital euro would allow the Eurosystem to be at the cutting edge of innovation.“¹ Auch Bundesbankpräsident *Jens Weidmann*² und der Gouverneur der Banque de France *François Villeroy de Galhau*³ zeigten sich offen für einen solchen Schritt, betonten aber zugleich die Rolle des privaten Sektors als Innovationsförderer.

[2] Spätestens mit diesen öffentlichen Stellungnahmen ist die Debatte um CBDC auch im Euroraum in eine präfinale Phase eingetreten. Auch wenn damit keine Abschaffung des Bargelds einhergehen und lediglich ei-

ne weitere Erscheinungsform des Geldes geschaffen werden soll, stellen sich neue Rechtsfragen im Geld-, Währungs- und Zahlungsdienstrecht von grundlegender Bedeutung. Dabei kommt es vielfach entscheidend darauf an, welches Umsetzungsmodell für CBDC letztlich gewählt wird.

II. Praktischer Bedarf und Einsatzfelder

[3] Als technische Basis für CBDC wird vor allem die Blockchain-Technologie diskutiert, durch die ein digitaler Euro beispielsweise als Euro-Token übertragen würde.⁴ Die Blockchain-Technologie wird bislang vor allem als Basis für privat emittierte „Kryptowährun-

* Der Autor *Omlor* (LL. M. (NYU), LL. M. Eur.) ist Mitherausgeber der *RD*i** und Direktor des Instituts für das Recht der Digitalisierung (Professur für Bürgerliches Recht, Handels- und Wirtschaftsrecht, Bankrecht sowie Rechtsvergleichung) an der Philipps-Universität Marburg; dort leitet er das BMJV-Forschungsprojekt „Blockchain und Recht“. Die Autorin *Birne* ist Doktorandin an diesem Institut und dem BMJV-Forschungsprojekt zugeordnet. Sämtliche Internetquellen wurden zuletzt am 27.10.2020 abgerufen.

1 *Lagarde*, Payments in a digital world, 10.9.2020, abrufbar unter: <https://beck-link.de/p5n6e>.

2 *Weidmann*, On the future of money and payments, 11.9.2020, abrufbar unter: <https://beck-link.de/36mfw>.

3 *de Galhau*, Preparing Europe Payments for the digital currency age, 11.9.2020, abrufbar unter: <https://beck-link.de/h7ab3>.

4 Vgl. *Brauneck* WM 2019, 1911 (1917).

gen“ wie Bitcoin oder Ether genutzt. Im Gegensatz zu herkömmlichen IT-Systemen zeichnet sich diese Technologie durch ihre kryptographische Sicherheit, verteilte Kontrolle und Effizienz aus. Durch sie kann beispielsweise das Risiko einer mehrfachen Ausgabe desselben Euro-Tokens (*Double Spending*) umgangen werden.⁵ Zahlungsvorgänge können zumindest pseudonymisiert stattfinden und somit je nach Ausgestaltung analog zum Bargeld ohne Identitätskenntnis. Liefer- und Zahlungsprozesse können programmiert und automatisiert werden, sodass beispielsweise ein festgelegter Geldbetrag in Euro-Token nur nach Erfüllung der durch den Smart Contract festgelegten Bedingung ausbezahlt wird.⁶ Die Abhängigkeit von Kunden zu Geschäftsbanken und mithin das Schuldnerisiko bei deren Zahlungsunfähigkeit würde je nach Modell entfallen. Durch Reduzierung bankspezifischer Risiken kann eine höhere Finanzstabilität geschaffen werden. Gerade Verbraucher erhielten ein sicheres Zahlungsmittel für die „digitale Wirtschaft der Zukunft“⁷.

[4] Die Abwicklung des internationalen Zahlungsverkehrs könnte deutlich effizienter, schneller und kostengünstiger gestaltet werden. Internationale Überweisungen des digitalen Euros in einen anderen Währungsraum könnten innerhalb von wenigen Sekunden und mit geringen bis gar keinen Transaktionskosten erfolgen. Hinzu kommt die Wettbewerbsfähigkeit gegenüber anderen Nationen, die ebenfalls an der Einführung von digitalem Zentralbankgeld arbeiten.⁸ Durch programmierte Zahlungsvorgänge könnten Euro-Zahlungen und andere Finanzdienstleistungen automatisch abgewickelt werden. Die Fehleranfälligkeit und der bürokratische Aufwand von manuellen Prozessen würden umgangen. Die Automatisierung führt zu einer Integration von Leistung und Gegenleistung. Gerade im internationalen Wirtschaftsverkehr fallen Leistung und Gegenleistung bisher oftmals auseinander. Durch den automatisierten Prozess könnte die Zahlung mit Eingang der Ware binnen Sekunden den Anbieter erreichen. Die programmierbare CBDC könnte zudem von Geräten wie Autos, Sensoren und Maschinen genutzt werden, die mit einem eigenen Wallet ausgestattet werden und somit direkt am Blockchain-Netzwerk teilnehmen können (Internet of Things).⁹ Der digitale Euro könnte die Digitalisierung der Industrie und der Maschinenökonomie vorantreiben und die Wettbewerbsfähigkeit europäischer Unternehmen fördern.¹⁰

[5] Die automatisierten Prozesse sollen ebenfalls einen effizienteren Wertpapiertransfer ermöglichen.¹¹ Aktuell werden hierfür mehrere Intermediäre benötigt. Über die Euro-Blockchain könnte ein Smart Contract eines digitalisierten Wertpapiers jedoch diese Funktion erfüllen und mithin die Intermediäre zumindest teilweise obsolet werden lassen. Die Übertragung des Wertpapier-Tokens würde automatisch und zeitgleich mit der Zahlung er-

folgen. Dies gilt ebenfalls für andere tokenisierbare Vermögensgegenstände.¹² Durch die direkte Übertragung ohne zwischengeschaltete Intermediäre werden Risiken aus deren Sphäre ausgeschaltet. Aufgrund transparenter Transaktionen sinkt ebenfalls das Manipulationsrisiko.¹³ Daten können nicht im Nachhinein verändert werden und werden nicht auf zentralen Servern gespeichert. Einen zentralen Anknüpfungspunkt für Hackerangriffe gibt es nicht.

III. Technisch-organisatorische Umsetzung

[6] Die genaue technische Umsetzung von digitalem Zentralbankgeld ist stark an mögliche Auswirkungen auf das Finanzsystem und Risiken für Nutzer gebunden.¹⁴ Es werden Datenschutzbedenken hinsichtlich des inter- und außereuropäischen Zahlungsverkehrs und dem möglichen Zugriff auf Transaktionsdetails von Zentralbanken geäußert.¹⁵ Damit einhergehend wird befürchtet, dass durch die Einführung von CBDC die schrittweise Abschaffung des Bargeldes vorangetrieben und mithin die einzig gänzlich anonyme Zahlungsweise unmöglich werde.¹⁶ Ökonomen sehen außerdem die Gefahr von „Bank Runs“, bei denen viele Kunden von Geschäftsbanken innerhalb kurzer Zeit ihr Geld auf Konten der Zentralbank überweisen und somit eine Liquiditätskrise der Geschäftsbanken auslösen. Durch den Abzug von Einlagen müssten sich die Banken über den Kapitalmarkt refinanzieren und es könnte zu einer Disintermediation des Bankensektors kommen.¹⁷ Im Zuge dieser Debatte haben sich zwei denkbare Modelle (mit Unterformen) der Umsetzung von digitalem Zentralbankgeld etabliert.¹⁸

1. Wholesale CBDC

[7] Wholesale CBDC steht für eine reine Interbanken-Währung für den Interbanken- und Wertpapierhandel.

-
- 5 Hanel/Michaelis, Digitales Zentralbankgeld als neues Instrument der Geldpolitik (12.3.2019), S. 4; weiterführend zur Technologie vgl. Sedlmeir RdZ 2020, 210 ff.
- 6 Zu den Motiven *FinTechRat*, Der digitale, programmierbare Euro (01.2020); *Bitkom*, Digitaler Euro auf der Blockchain (2020).
- 7 *Bankenverband*, Europas Antwort auf Libra: Potenzial und Bedingungen eines programmierbaren Euro (17.6.2020), abrufbar unter: <https://beck-link.de/mrk3r>.
- 8 ECB, Report on a digital Euro (10/2020), S. 14, abrufbar unter: <https://beck-link.de/8krx4>; zu den internationalen Entwicklungen *FinTechRat* (Fn. 6) S. 17.
- 9 *FinTechRat* (Fn. 6) S. 4, 7; *Bitkom* (Fn. 6) S. 11 f.
- 10 *FinTechRat* (Fn. 6) S. 17.
- 11 Ausführlich *Bitkom* (Fn. 6) S. 12 f.
- 12 *FinTechRat* (Fn. 6) S. 5.
- 13 Vgl. Klein/Groß/Sandner ifo Schnelldienst 3/2020, S. 39 (41).
- 14 ECB (Fn. 8) S. 16 f.
- 15 *Bitkom* (Fn. 6) S. 17 f.
- 16 *Bitkom* (Fn. 6) S. 17 f.
- 17 *Bankenverband* (Fn. 7); ausführliche Diskussion Bindseil, Tiered CBDC and the financial system, ECB Working Paper Series No 2351, 2020, S. 8 ff.; Klein/Groß/Sandner ifo Schnelldienst 3/2020, S. 39 (44).
- 18 Vgl. *FinTechRat* (Fn. 6) S. 9 ff; *Bitkom* (Fn. 6) S. 8.

Verbraucher und Nichtbanken sind von CBDC ausgeschlossen. Ziel ist die Förderung des grenzüberschreitenden Zahlungsverkehrs zwischen Finanzinstituten und die Abwicklung von Wertpapiergeschäften. Durch Einführung von Wholesale CBDC würde das bereits bestehende zweistufige Geldsystem beibehalten und ein effizienteres Interbanken-Zahlungssystem etabliert werden, gerade wenn auch der Wertpapierhandel in das Blockchain-Netzwerk integriert wird.¹⁹ Der Bundesverband deutscher Banken fordert beispielsweise die Ausgabe des digitalen Euros nur durch Kreditvergabe der Zentralbank an die Geschäftsbanken.²⁰

2. Retail CBDC

[8] Beim Retail CBDC wird auch Endkunden, mithin Verbrauchern und Nichtbanken, der direkte Zugang zur CBDC ermöglicht. Es würde neben Bar- und Buchgeld als Zahlungsmittel Verwendung finden. Die Effizienz des Zahlungsverkehrs würde möglicherweise gesteigert und der Rückgang des Bargeldes kompensiert. Zudem wäre der Zugang zu risikofreiem Geld ohne Abhängigkeit von der Solvenz einer Geschäftsbank sichergestellt, sowie die Konkurrenzfähigkeit gegenüber privat emittierten Blockchain-basierten Zahlungsmitteln.²¹ Im Zusammenhang mit Retail CBDC werden drei Modelle diskutiert. Zudem stellte die EZB ein eigenes Retail CBDC Modell vor.

a) Das direkte Modell

[9] Das direkte Modell erlaubt es jedermann, ein Konto direkt bei der Zentralbank zu eröffnen und den digitalen Euro als direkte Forderung gegenüber der EZB zu halten. Ein Konto auf Blockchain-Basis stellt jedoch kein Bankkonto im herkömmlichen Sinn dar, sondern ein sog. „Wallet“, eine digitale Brieftasche. Die CBDC könnte direkt von einem Wallet zum anderen übertragen werden. Die Verwaltung und die Kundenidentitäts- bzw. Anti-Geldwäsche-Prüfung lägen dann ebenfalls in der direkten Verantwortung der EZB. Dies würde jedoch zum einen zur Überschreitung des Kerngeschäfts der EZB führen und zum anderen erhebliche Kosten verursachen. Der Bankenverband fürchtet dadurch eine Überlastung der Zentralbanken, sowie den Weg in ein Vollgeldsystem, in dem der Zahlungsverkehr ausschließlich durch digitales Zentralbankgeld durchgeführt wird und die Geschäftsbanken somit Funktionen verlieren.²²

b) Das indirekte Modell

[10] Das indirekte Modell kommt indes nicht ohne Zwischenschaltung von Intermediären aus. Endkunden halten ein Konto direkt bei anderen Finanzinstituten und haben gegen diese einen Zahlungsanspruch auf „inter-

mediären“ digitalen Euro, der vom jeweiligen Intermediär mit dem originären digitalen Euro gedeckt sein muss. Dafür stellt der Intermediär dem Nutzer einen Vermögenswert zur Verfügung, beispielweise eine Einlage, E-Geld oder Wertpapiere, der vollständig mit Zentralbankgeld besichert ist (indirektes CBDC oder iCBDC). Er hat lediglich Zugriff auf den Vermögenswert, nicht aber auf die CBDC. Der Nutzer ist vertraglich an den Intermediär gebunden, steht jedoch in keinem Rechtsverhältnis zur Zentralbank. Der Intermediär hingegen hält ein Zentralbankkonto bei der Zentralbank.²³

c) Das hybride Modell

[11] Beim hybriden Modell erhält der Endkunde einen direkten Zahlungsanspruch auf digitalen Euro gegen die EZB. Jedoch wird dieser Zahlungsanspruch über einen treuhänderisch agierenden Intermediär geltend gemacht. Dieser verwaltet die Transaktionen und erlaubt den indirekten Zugriff auf den digitalen Euro. Die Intermediäre könnten beispielsweise Zahlungsdienstleister im Sinne der Zweiten EU-Zahlungsdiensterichtlinie (PSD2)²⁴ sein und Zahlungsauslöse- oder Kontoinformationsdienste bereitstellen, die über das Zentralbankkonto des Nutzers ausgeführt werden.²⁵ Der Nutzer stünde mithin in einem Rechtsverhältnis mit der Zentralbank über das Zentralbankkonto. Mit den Zahlungsdienstleistern würde ein Vertragsverhältnis über die Zahlungsdienstleistungen bestehen. Zum anderen könnten technische Dienstleister die Intermediärsfunktion übernehmen, die Dienstleistungen zur Speicherung und Übertragung von CBDC anbieten. In diesem Zusammenhang wäre ebenfalls an einen Wallet-Anbieter zu denken, der den Private Key des Nutzers verwahrt. Diese Konstellation würde ebenfalls zu einer vertraglichen Beziehung zwischen dem Nutzer und dem technischen Dienstleister führen, sowie zu einem Rechtsverhältnis zwischen dem Benutzer und der Zentralbank.²⁶ Trägt der technische Dienstleister lediglich zur Erbringung der Zahlungsdienste bei, gelangt jedoch zu keiner Zeit in den Besitz der zu transferierenden Geldbeträge, ist er vom Anwendungsbereich der PSD2 ausgeschlossen.²⁷ Dies

¹⁹ Klein/Groß/Sandner ifo Schnelldienst 3/2020, S. 39 (43).

²⁰ Bankenverband (Fn. 7).

²¹ Zu den Vorteilen Bindseil (Fn. 17) S. 8 ff.

²² Bankenverband (Fn. 7).

²³ Hess, Regulating Central Bank Digital Currencies: Towards a Conceptual Framework, 2020, S. 13 f.

²⁴ Richtlinie (EU) 2015/2366 des Europäischen Parlaments und des Rates vom 25. November 2015 über Zahlungsdienste im Binnenmarkt, zur Änderung der Richtlinien 2002/65/EG, 2009/110/EG und 2013/36/EU und der Verordnung (EU) Nr. 1093/2010 sowie zur Aufhebung der Richtlinie 2007/64/EG.

²⁵ Hess, Regulating Central Bank Digital Currencies: Towards a Conceptual Framework, S. 10 f.

²⁶ Hess, Regulating Central Bank Digital Currencies: Towards a Conceptual Framework, S. 12 f.

²⁷ Richtlinie (EU) 2015/2366 (Fn. 24), Art. 3 j.

wäre der Fall, wenn der technische Dienstleister lediglich den technischen Zugang zur CBDC ermöglichen würde.

d) Das Modell der EZB

[12] Die EZB veröffentlichte im Dezember 2019 ein Retail CBDC-Modell auf DLT-Basis, genauer auf der Corda-Blockchain.²⁸ Der digitale Euro soll an die breite Öffentlichkeit als Zahlungsmittel ausgegeben werden, jedoch über Intermediäre mit zweistufiger Verzinsung. Anstatt die Nutzer des digitalen Euros direkt zu betreuen, nutzt die Zentralbank Intermediäre, um die CBDC zur Verfügung zu stellen und um diese zu verwalten. Sie wickeln Transaktionen im Namen ihrer Kunden ab und bieten ihnen Verwahrungsdienstleistungen an. Die Intermediäre verwahren den privaten Schlüssel der Nutzer zur Initiierung von Zahlungen, da diese keinen direkten Zugang zum Blockchain-Netzwerk haben.²⁹ Die zweifache Verzinsung soll einem Bank Run bzw. der Disintermediation des Bankensektors insoweit entgegenwirken, dass keine großen Summen des digitalen Euros gehalten werden. Die EZB hat das ausschließliche Recht zur Ausgabe und Rücknahme des digitalen Euros.

IV. Unionaler Rechtsrahmen

[13] Die Einführung von CBDC wirft unionsrechtlich kompetenzielle Fragen auf; sie betrifft aber auch die Vereinbarkeit mit dem geltenden Sekundärrecht.

1. Primärrechtliche Zulässigkeit

[14] Die Ausgabehoheit von Geldzeichen durch die EZB ist in Art. 128 AEUV geregelt, wonach die Europäische Zentralbank das ausschließliche Recht hat, die Ausgabe von Euro-Banknoten und Euro-Münzen innerhalb der Union zu genehmigen. Zudem setzt Art. 128 I 3 AEUV die von der Europäischen Zentralbank und den nationalen Zentralbanken ausgegebenen Banknoten als einziges gesetzliches Zahlungsmittel der Union fest und statuiert mithin eine gesetzliche Pflicht zur Annahme von Euro-Geldzeichen.³⁰ Zunächst ist festzustellen, dass keine Norm im AEUV oder in der ESZB/EZB-Satzung ersichtlich ist, die ausdrücklich die Ausgabe anderer Gelderscheinungsformen außer Euro-Banknoten als gesetzliches Zahlungsmittel ausschließen würde.³¹ Einer primärrechtlichen Zulässigkeit zur Einführung des digitalen Euros könnte jedoch entgegenstehen, wenn Art. 128 AEUV andere Formen der Geldausgabe als die dort genannten sperren würde.

[15] Dies wäre der Fall, wenn es sich bei Art. 128 AEUV um eine abschließende Regelung für die Geldversorgung durch die EZB handelte. Dazu muss Art. 128 AEUV systematisch im Kontext zu Art. 127 AEUV be-

trachtet werden, welcher die Ziele und Aufgaben des ESZB festlegt und somit die Kernaussagen der europäischen Währungsverfassung beinhaltet.³² Nach Art. 127 I AEUV ist primäres Ziel des ESZB die Gewährleistung der Preisstabilität innerhalb der Union. Zur Erreichung dieses Zieles soll der Aufgabenkatalogs des zweiten Absatzes dienen.³³ Hingegen demnach etwa die Funktionsfähigkeit der Zahlungssysteme von einer reinen Bargeldversorgung ab, ließe sich daraus eine Sperrwirkung für andere Formen der Geldausgabe ableiten. Ob die Bargeldausgabe erforderlich für die Funktionsfähigkeit der Zahlungssysteme ist, bestimmt sich nach der Nachfrage für Bargeld und auch der Verbreitung von alternativen Geldzahlungsformen.³⁴ Die immer weiter zurückgehende Verbreitung von Bargeld und die zunehmende Verwendung von Buchgeld³⁵ spricht indes gegen die Annahme, die Funktionsfähigkeit der Zahlungssysteme hinge vom Bargeld als einzige Gelderscheinungsform ab. Ein Grundrecht auf Zurverfügungstellung von Bargeld als einzige Gelderscheinungsform existiert ebenso wenig wie eine grundrechtlich geschützte Wahlfreiheit zwischen den verschiedenen Gelderscheinungsformen.³⁶ Selbst wenn sich eine etwaige Pflicht zur Bargeldausgabe aus Art. 128 AEUV ergeben sollte, steht diese der Einführung einer weiteren Gelderscheinungsform nicht entgegen, da mit der Einführung von CBDC gerade nicht die Abschaffung des Bargeldes einhergeht. Es ist mithin nicht von einer Sperrwirkung des Art. 128 AEUV gegenüber anderen Gelderscheinungsformen auszugehen.

2. Sekundärrechtliche Zulässigkeit

[16] In Art. 10 und 11 der Verordnung über die Einführung des Euro (im Folgenden EuroEinfVO)³⁷ wird festgelegt, dass nur auf Euro lautenden Banknoten als einzige in allen diesen Mitgliedstaaten die Eigenschaft eines gesetzlichen Zahlungsmittels zukommt. Die sekundärrechtlichen Regelungen zum gesetzlichen Annahmewang beschränken sich gerade auf verkörperte Geldzeichen, worunter sich digitales Zentralbankgeld

²⁸ ECB, Exploring anonymity in central bank digital currencies, 2019, abrufbar unter: <https://beck-link.de/sr52v>.

²⁹ ECB (Fn. 28) S. 8 f.

³⁰ MüKoBGB/Grundmann, 8. Aufl. 2019, § 245 Rn. 50 f.

³¹ ECB (Fn. 8) S. 25.

³² Schwarze/Becker/Hatje/Schoo/Wutscher, EU-Kommentar, 4. Aufl. 2019, Art. 127 AEUV Rn. 3; Vedder/Heintschel von Heinegg/Rodi, Europäisches Unionsrecht, 2. Aufl. 2018, Art. 127 AEUV Rn. 1.

³³ Grabitz/Hilf/Nettesheim/Griller, Das Recht der Europäischen Union (Stand: 70. EL Mai 2020), Art. 127 AEUV Rn. 31.

³⁴ Vgl. Omlor WM 2015, 2297 (2299).

³⁵ Deutsche Bundesbank, Wachstum unbarer Zahlungen setzt sich 2018 fort, 26.7.2019, abrufbar unter: <https://beck-link.de/n7m54>; dies., Zahlungsverkehrs- und Wertpapierabwicklungsstatistiken in Deutschland 2014–2018, Juli 2019, abrufbar unter: <https://beck-link.de/3e7zb>.

³⁶ Vgl. Omlor WM 2015, 2297 (2301).

³⁷ Verordnung (EG) Nr. 974/98 vom 3.5.1998 über die Einführung des Euro, Abl. EU Nr. L139 S. 1 vom 11.5.1998.

nicht subsumieren lässt. Um einen digitalen Euro in Form eines gesetzlichen Zahlungsmittels etablieren zu können, müsste zumindest die EuroEinfVO insofern angepasst werden.³⁸ Nach Ansicht der EZB könnte auf Grundlage von Art. 133 AEUV ein Sekundärgesetz verabschiedet werden, das die Bedingungen für die Ausgabe eines digitalen Euros als gesetzliches Zahlungsmittel festlegt.³⁹

3. Kompetenzgrundlage

[17] Als Kompetenzgrundlage kommt Art. 3 I lit. c i. V. m. Art. 127 ff. AEUV in Betracht. Art. 3 I lit. c AEUV schreibt der Union die ausschließliche Zuständigkeit für die Währungspolitik zu. Deren Inhalt orientiert sich am Aufgabenkatalog der Art. 127 ff. AEUV.⁴⁰ In Art. 127 II Spiegelstrich 4 AEUV wird dem ESZB die Förderung des reibungslosen Funktionierens der Zahlungssysteme zugeschrieben. Dessen Konkretisierung in Art. 22 ESZB/EZB-Satzung beinhaltet keine Kompetenz der EZB, die Form des Euros zu bestimmen bzw. eine neue Form zu etablieren und in Umlauf zu bringen.⁴¹ Der Katalog des Art. 127 II AEUV stellt jedoch keinen *numerus clausus* dar, vielmehr bildet er lediglich die grundlegenden Aufgaben ab und schließt die Übernahme von anderen Aufgaben gerade nicht aus.⁴² Art. 3 I lit. c AEUV umfasst die ausschließliche Zuständigkeit der Union im Bereich der Währungspolitik in ihrer Gesamtheit, die anhand ihrer Zielsetzung ausgelegt wird.⁴³ Daraus kann ebenfalls die Kompetenz zur Einführung eines Euros auf Blockchain-Basis abgeleitet werden. Da die Währungspolitik der Euro-Staaten dem Europäischen System der Zentralbanken obliegt, läge die Einführung des digitalen Euros als Annex zu Art. 127 II AEUV ebenfalls in dessen Kompetenzbereich.⁴⁴

[18] Die EZB selbst geht davon aus, Art. 127 II AEUV i. V. m. Art. 17, 20 oder 22 ESZB/EZB-Satzung könnte abhängig von der gewählten Gestaltungsform des digitalen Euros als Rechtsgrundlage für die Ausgabe dienen.⁴⁵ Wird der digitale Euro lediglich als geldpolitisches Instrument ähnlich der Zentralbankreserven ausgegeben, kommt als Rechtsgrundlage in der Tat Art. 127 II AEUV i. V. m. Art. 20 S. 1 ESZB/EZB-Satzung in Betracht.⁴⁶ Wenn der digitale Euro hingegen jedermann über Konten bei der EZB direkt zur Verfügung gestellt wird, läge zumindest für die Eröffnung der Konten Art. 127 II AEUV i. V. m. Art. 17 ESZB/EZB-Satzung näher.⁴⁷ In Betracht kommt ebenfalls Art. 127 II AEUV i. V. m. Art. 22 ESZB/EZB-Satzung, würde der digitale Euro lediglich über eine spezielle Zahlungsinfrastruktur, die nur berechtigten Teilnehmern zugänglich ist, ausgegeben werden.⁴⁸ Wird der digitale Euro den Euro-Banknoten als gesetzliches Zahlungsmittel gleichgestellt, wäre Art. 128 AEUV i. V. m. Art. 16 S. 1 ESZB/EZB-Satzung die geeignete

Rechtsgrundlage.⁴⁹ Denn das Recht zur Ausgabe von Euro-Banknoten könnte ebenfalls das Recht zur Bestimmung des Formats der Euro-Banknoten umfassen.⁵⁰

4. Zwischenergebnis

[19] In Übereinstimmung mit den Einschätzungen der EZB wäre eine primärrechtliche Anpassung aufgrund einer vorliegenden Kompetenzgrundlage nicht notwendig. Jedoch würde eine Ergänzung von Art. 128 AEUV um einen dritten Absatz oder eine Textergänzung in der ESZB-Satzung für mehr Rechtsklarheit sorgen.⁵¹

V. Rechtsnatur

1. Währungsrechtliche Einordnung

[20] Der Begriff der Währung steckt den Anwendungsbereich einer hoheitlichen Geldverfassung eines Staates ab und sorgt für ein einheitliches Geldsystem.⁵² Der Währungsbegriff besteht mithin aus zwei Komponenten, dem abstrakten und dem konkreten Währungsbegriff, die jedoch eine notwendige Einheit bilden. Abstrakt bildet die Währung die ideelle Einheit eines Geldsystems, konkret spiegelt sie die Geldverfassung eines Staates wider und ist mithin staatlich legitimiert und geographisch bestimmt.⁵³ Folglich ist die Währung ein auf staatlichem Recht aufbauendes System und mithin Rechtsbegriff.⁵⁴ Der Blockchain-basierte Euro könnte jedenfalls nur unter diesen Währungsbegriff fallen, wenn er in die Geldverfassung der Mitgliedsstaaten der Europäischen Währungsunion aufgenommen würde. Zwar sieht Art. 128 AEUV bisher lediglich die Ausgabe von Euro-Banknoten und Euro-Münzen vor, jedoch stellt dies – wie bereits erläutert⁵⁵ – grundsätzlich kein

³⁸ Vgl. Möslin/Omlor/*ders./Spiegel*, FinTech-Handbuch, 2019, § 19 Rn. 13; Omlor ZHR 183 (2019), 294 (338 f.).

³⁹ ECB (Fn. 8) S. 24.

⁴⁰ Schwarze/Becker/Hatje/Schoo/Pelka, EU-Kommentar, Art. 3 AEUV Rn. 11; Vedder/Heintschel von Heinegg/Vedder, Europäisches Unionsrecht, Art. 3 AEUV, Rn. 7; von der Groeben/Schwarze/Hatje/Obwexer, Europäisches Unionsrecht, 7. Aufl. 2015, Art. 3 AEUV Rn. 18.

⁴¹ Zum Regelungsinhalt von der Groeben/Schwarze/Hatje/Karpf, Europäisches Unionsrecht, Satzung ESZB/EZB Art. 22 Rn. 3 ff.

⁴² Schwarze/Becker/Hatje/Schoo/Wutscher, EU-Kommentar, Art. 127 AEUV, Rn. 14; von der Groeben/Schwarze/Selmayr, Europäisches Unionsrecht, Art. 127 AEUV Rn. 9 f.

⁴³ Vgl. EuGH NJW 2013, 29 Rn. 53.

⁴⁴ Möslin/Omlor/*ders./Spiegel*, FinTech-Handbuch, § 19, Rn. 14.

⁴⁵ ECB (Fn. 8) S. 24.

⁴⁶ ECB (Fn. 8) S. 24.

⁴⁷ ECB (Fn. 8) S. 24.

⁴⁸ ECB (Fn. 8) S. 24.

⁴⁹ ECB (Fn. 8) S. 24.

⁵⁰ ECB (Fn. 8) S. 25.

⁵¹ Möslin/Omlor/*ders./Spiegel*, FinTech-Handbuch, § 19, Rn. 14; Omlor ZHR 183 (2019), 294 (338 f.).

⁵² Möslin/Omlor/*ders./Spiegel*, FinTech-Handbuch, § 19, Rn. 12; Omlor ZHR 183 (2019), 294 (307).

⁵³ Zum zweigliedrigen Währungsbegriff Omlor, Geldprivatrecht, 2014, S. 158; Omlor JZ 2017, 754 (758 f.).

⁵⁴ Hahn/Häde, Währungsrecht, 2010, § 2 Rn. 2.

⁵⁵ Siehe oben, sub III. Rechtsrahmen.

Hindernis für die Ausweitung der europäischen Währungsverfassung auf den digitalen Euro dar.

2. Geldrechtliche Einordnung

[21] Eng mit der währungsrechtlichen Einordnung des digitalen Euros verbunden ist dessen geldrechtlicher Charakter. Mangels Legaldefinition muss Geld im Rechtssinne zum einen an der *lex lata* gemessen werden, um Rechtssicherheit gewährleisten zu können, und zum anderen flexibel in Hinblick auf gesellschaftliche Entwicklungen sein. Anhand dieser Kriterien hat sich der zweigliedrige Geldbegriff entwickelt, der aus Geld im konkreten Sinne und Geld im abstrakten Sinne besteht.⁵⁶

a) Geld im konkreten Sinne

[22] Mit Geld im konkreten Sinne ist das als gesetzliche Zahlungsmittel anerkannte Bargeld gemeint. Voraussetzung für die Einordnung als Geld im konkreten Sinne ist mithin dessen Anerkennung als gesetzliches Zahlungsmittel, die allgemeine Anerkennung als Tauschmittel sowie dessen Verkörperung.⁵⁷ Im Euro-Raum sind nur auf Euro lautende Banknoten das einzige unbeschränkte gesetzliche Zahlungsmittel. Die Euro-EinfVO kann jedoch insoweit erweitert werden, als dass auch CBDC als gesetzliches Zahlungsmittel anerkannt wird. Auch die EZB ist der Ansicht, dass die Anerkennung des digitalen Euros als gesetzliches Zahlungsmittel wünschenswert sei, da dieser ansonsten lediglich die Akzeptanz eines herkömmlichen elektronischen Zahlungsmittels erfahren würde.⁵⁸ Die allgemeine Anerkennung als Tauschmittel fordert den Einsatz des konkreten Tauschmittels auf universelle Weise. Findet der digitale Euro Einzug in die Währungsverfassung und wird als gesetzliches Zahlungsmittel mit gesetzlichen Annahmezwang anerkannt, spricht bereits dieser normative Akt für seine tatsächliche Verwendung als universelles Tauschmittel.

[23] CBDC kann jedoch nicht das Merkmal der Verkörperung erfüllen. Zu denken wäre an eine Erweiterung des konkreten Geldbegriffs im Zuge der fortschreitenden Entmaterialisierung des Geldes. Die enge Gelddefinition, die strikt am Erfordernis der Körperlichkeit festhält, entspricht zwar der klassischen Auffassung in der Rechtswissenschaft.⁵⁹ Fraglich ist jedoch, ob die Verkörperung im traditionellen Sinn als Anforderung an den konkreten Geldbegriff noch zeitgemäß ist. Der konkrete Geldbegriff ist strukturell wegen der Anknüpfung an eine Verkörperung weniger entwicklungs offen als sein abstraktes Gegenüber formuliert. Zu denken wäre an eine Extension des Begriffs der Verkörperung, ohne am Erfordernis einer räumlich-physischen Ausdehnung festzuhalten. Verkörperung könnte auch die

Abgrenzbarkeit einer bestimmten digitalen Einheit bedeuten, so dass über sie verfügt werden kann und sie zudem nicht vervielfältigbar ist.⁶⁰ Anknüpfungspunkt eines derart funktionalen Begriffs der Verkörperung wäre die eindeutige Zuordnungsmöglichkeit und Verfügungsmacht über einen Gegenstand. Die Zuordnung des digitalen Euros erfolgt über das Blockchain-Netzwerk anstatt über eine räumliche Greifbarkeit. Eine eindeutige und absolute Verfügung wäre technisch ebenfalls möglich. Als Vorbild könnte die Sachfiktion für elektronische Wertpapiere in § 2 Abs. 3 eWpG-E⁶¹ dienen. Alternativ könnte neben das Tatbestandsmerkmal der Verkörperung das Tatbestandsmerkmal der nicht-körperlichen Gegenstände treten. Das Erfordernis der Verkörperung könnte auch gänzlich aufgehoben werden. Dann würde der konkrete Geldbegriff nur noch aus den Voraussetzungen der Anerkennung als gesetzliches Zahlungs- und allgemeines Tauschmittel bestehen.

b) Geld im abstrakten Sinne

[24] Geld im abstrakten Sinne setzt demgegenüber gerade nicht die Anerkennung als gesetzliches Zahlungsmittel oder eine Verkörperung voraus. Jedoch bedarf es einer zumindest normativen Anerkennung in der Rechtsordnung, sowie der Verwendung als Universaltauschmittel mit Wertmaßcharakter.⁶² Der abstrakte Geldbegriff unterliegt mithin keinem hoheitlichen Schöpfungsakt bzw. einem gesetzlichen Annahmezwang.⁶³ Das Bargeld ist anhand dieser Definition nicht nur dem konkreten, sondern ebenfalls dem abstrakten Geldbegriff zuzuordnen.⁶⁴ Der digitale Euro dürfte alle Merkmale des abstrakten Geldbegriffs erfüllen. Die Aufnahme in die Währungsverfassung der Union oder die Anerkennung als gesetzliches Zahlungsmittel würde weit über die geforderte normative Anerkennung hinaus gehen. Somit würde der digitale Euro dem abstrakten Geldbegriff genügen. Konkret könnte der digitale Euro zwei etablierten Anwendungsfällen des abstrakten Geldbegriffs unterfallen.

aa) Buchgeld

[25] Das Buchgeld ist nach zutreffender und im Vordergrund befindlicher Auffassung als Geld im Rechtssin-

⁵⁶ Weiterführend Omlor, Geldprivatrecht, S. 100.

⁵⁷ Omlor, Geldprivatrecht, S. 100.

⁵⁸ ECB (Rn. 8) S. 33.

⁵⁹ Beispielsweise Knapp, Staatliche Theorie des Geldes, 1923, S. 6; Gerber, Geld und Staat, 1960, S. 29 ff., S. 52 ff.; Mann, Das Recht des Geldes, 1960, S. 5 ff.

⁶⁰ Vgl. John BKR 2020, 76 (78).

⁶¹ BMJV/BMF, Entwurf eines Gesetzes zur Einführung von elektronischen Wertpapieren (11.8.2020), abrufbar unter: <https://beck-link.de/d7fmx>.

⁶² Omlor ZHR 183 (2019), 294 (306); ausführlich Omlor, Geldprivatrecht, S. 98.

⁶³ Staudinger/Omlor, 2016, Vorbem. A66 zu §§ 244 ff.

⁶⁴ Vgl. Omlor WM 2015, 2297 (2302).

ne anzuerkennen.⁶⁵ Es stellt die nicht körperliche Form einer Geldsumme dar, die anstatt mit körperlichen Geldzeichen in Büchern oder anderen Datenträgern verzeichnet wird.⁶⁶ Es wird in der Gestalt einer Geldforderung als Guthaben bei Banken gehalten und kann jederzeit zu Zahlungszwecken verwendet werden.⁶⁷ Bei CBDC müsste demnach eine Forderung gegen einen Emittenten bestehen. Die CBDC würde von einer zentralen Ausgabestelle, der EZB, emittiert werden. Beim Wholesale CBDC steht es lediglich den Geschäftsbanken zu, ein Konto bzw. Wallet bei der Zentralbank zu führen und den digitalen Euro zu verwenden. Eine Forderung gegen die Zentralbank als Emittentin des digitalen Euros würde indes bestehen, da das digitale Zentralbankgeld eine Verbindlichkeit der Zentralbank und eine Forderung der Geschäftsbanken darstellt. Ähnliches gilt für das indirekte Modell des Retail CBDC. Im Unterschied zum Wholesale CBDC besteht beim direkten oder hybriden Retail CBDC eine direkte Forderung von Endkunden gegen die Zentralbank, die entweder vom Endkunden selbst oder über einen Intermediär geltend gemacht werden kann. Hier würde die Ausgabe des digitalen Euros analog zum traditionellen Zentralbankgeld ebenfalls eine Verbindlichkeit der Zentralbank und mithin eine Forderung der Endkunden darstellen.⁶⁸ Die Euro-Token würden ein Guthaben abbilden, das jederzeit zu Zahlungszwecken verwendet werden könnte. Unter diesen Aspekten könnte CBDC die Buchgeld-eigenschaft zukommen.

[26] Wird das digitale Zentralbankgeld analog zum Bargeld als gesetzliches Zahlungsmittel anerkannt und einem gesetzlichen Annahmewang unterstellt, kann es zwar nicht als Buchgeld im traditionellen Sinne eingeordnet werden. Das Buchgeld stellt nämlich gerade kein gesetzliches Zahlungsmittel dar, sondern nur einen Anspruch auf ein gesetzliches Zahlungsmittel, wodurch ebenfalls nicht von einem gesetzlichen Annahmewang ausgegangen werden kann.⁶⁹ Jedoch würde es sich gewissermaßen um ein „Buchgeld +“ handeln, das als Plus um einen gesetzlichen Annahmewang erweitert ist.

bb) E-Geld

[27] Das E-Geld als Sonderform des Buchgeldes⁷⁰ fällt ebenfalls unter den abstrakten Geldbegriff. Nach der Legaldefinition in § 1 II 3 ZAG ist E-Geld „jeder elektronisch, darunter auch magnetisch, gespeicherte monetäre Wert in Form einer Forderung an den Emittenten, der gegen Zahlung eines Geldbetrags ausgestellt wird, um damit Zahlungsvorgänge im Sinne des § 675 f Absatz 4 Satz 1 des Bürgerlichen Gesetzbuchs durchzuführen, und der auch von anderen natürlichen oder juristischen Personen als dem Emittenten angenommen wird.“ E-Geld wird auch als Buchgeld mit elektronischer Speicherung beschrieben.⁷¹ Es wird entweder als

Guthaben auf einem vom E-Geld-Emittenten betriebenen Server (z. B. PayPal⁷², Amazon Pay⁷³) oder auf einer Geldkarte gespeichert. Ebenso wie das Buchgeld stellt E-Geld eine Forderung gegen den E-Geld-Emittenten dar. Grundsätzlich erhält der Zahlende einen Anspruch auf Rückumwandlung des vorausgezählten E-Geldes in reguläres Buchgeld in Form einer Rücküberweisung auf sein Konto.⁷⁴

[28] Die EZB kann allenfalls dann als E-Geld-Emittentin agieren, sofern sie nicht in ihrer Eigenschaft als Währungsbehörde handelt (§ 1 II 1 Nr. 3 ZAG). Würde der digitale Euro in die Währungsverfassung der EU aufgenommen und die EZB diesen mithin in ihrer hoheitlichen Funktion als Währungsbehörde ausgeben, würde sie von vornherein vom Anwendungsbereich des ZAG ausgeschlossen sein, da dieses lediglich eine Privilegierung für nicht hoheitliches Handeln eines Hoheitsträgers enthält.⁷⁵ Für die Ausgabe des digitalen Euros als E-Geld bedarf die EZB in diesem Fall einer gesetzlichen Ermächtigung. Es ist dann Aufgabe des Gesetzgebers, eine gesonderte Regulierung oder sogar eine etwaige Beaufsichtigung für diese Konstellation zu treffen.⁷⁶ Für das direkte Modell der Retail CBDC würde dies bedeuten, dass das ZAG und damit das Zahlungsdienstrecht keine Anwendung finden. Die EZB würde als Währungsbehörde den digitalen Euro ohne Zwischenschaltung gegenüber den Nutzern ausgeben und verwalten. Die Rechtsbeziehung zwischen EZB und Nutzer kann jedoch aufgrund des hoheitlichen Handelns der EZB nicht unter den Anwendungsbereich des ZAG fallen. Beim indirekten Modell könnte das Zahlungsdienstrecht zumindest im Verhältnis zwischen Nutzer und Intermediär anwendbar sein, zumindest wenn dieser Zahlungsdienstleister bzw. E-Geld-Emittent i. S. d. ZAG ist. Dies gilt ebenfalls für das hybride Modell und das EZB-Modell, da auch hier je nach Ausgestaltung im Verhältnis zwischen Nutzer und Intermediär das Zahlungsdienstrecht Anwendung finden kann.

[29] Unabhängig vom persönlichen Anwendungsbereich des E-Geld-Rechts stellt sich die Frage, ob der digitale Euro überhaupt als E-Geld ausgestaltet werden

⁶⁵ Vgl. Staudinger/Omlor, Vorbem. A71 zu §§ 244 ff.; Omlor, Geldprivatrecht S. 105; Schimansky/Bunte/Lwowski/Haug, BankR-Hdb., 5. Aufl. 2017, § 123 Rn. 47 ff.

⁶⁶ Hahn/Häde, Währungsrecht, Rn. 23.

⁶⁷ Omlor, Geldprivatrecht, S. 104.

⁶⁸ Vgl. Hanell/Michaelis (Fn. 5) S. 7.

⁶⁹ Schimansky/Bunte/Lwowski/Schefold, BankR-Hdb., § 115 Rn. 51.

⁷⁰ Staudinger/Omlor, 2020, § 675 c Rn. 6; Überblick zur umstrittenen Rechtsnatur bei Casper/Terlau/Terlau, ZAG, 2. Aufl. 2020, § 1 Rn. 202 ff.

⁷¹ Staudinger/Omlor, Vorbem A152 zu §§ 244 ff.

⁷² Vgl. MüKoHGB/Herresthal, Band 6, 4. Aufl. 2019, Teil 1A Rn. 74 ff.

⁷³ Staudinger/Omlor, § 675 i Rn. 41.

⁷⁴ MüKoBGB/Casper, 8. Aufl. 2020, § 675 c Rn. 30.

⁷⁵ Casper/Terlau/Terlau, ZAG, § 1 Rn. 192.

⁷⁶ Casper/Terlau/Terlau, ZAG, § 1 Rn. 192.

kann und damit der sachliche Anwendungsbereich eröffnet ist. Der monetäre Wert des digitalen Euros ergibt sich bereits aus dessen Funktion als Zahlungsbzw. Tauschmittel.⁷⁷ Eine Forderung gegen den Emittenten ist dann gegeben, wenn sich der Emittent gegenüber dem Kunden verpflichtet, die herausgegebene Werteinheit gegen gesetzliches Zahlungsmittel zurückzutauschen. Die Parteien müssten demnach vertraglich vereinbaren, dass der Token-Inhaber zum Rücktausch des Tokens in ein gesetzliches Zahlungsmittel berechtigt ist (vgl. § 33 I 2 ZAG).⁷⁸ Im Übrigen gelten die allgemeinen Anforderungen an Buchgeld. Der Euro-Token dürfte nur Zug-um-Zug gegen (Voraus-)Zahlung eines Geldbetrags ausgestellt werden. Der Begriff des Geldbetrags umfasst Banknoten und Münzen, Giralgeld oder E-Geld.⁷⁹ Fasst man den Begriff des „Ausstellens“ weit, ist die Einräumung der Verfügungsmacht über die geldwerte Einheit hierfür ausreichend.⁸⁰ Die elektronische Speicherung soll den Anspruch des E-Geld-Inhabers auf eine bestimmte Leistung gegen den Emittenten festhalten. Laut BaFin kann es sich dabei um jedes elektronische Speichermedium unabhängig von Ort und Form der Speicherung handeln.⁸¹ Bei CBDC werden nicht die Einheiten selbst lokal gespeichert, sondern lediglich die Information über ein bestimmtes Guthaben einer Blockchain-Adresse dezentral auf der Blockchain. Für die elektronische Speicherung ist es jedoch ausreichend, dass durch die Speicherung festgehalten wird, wie viele monetäre Werte einem Kunden zustehen. Dies ist über die gespeicherten Informationen auf der Blockchain gerade möglich. Die für die Bestimmung des monetären Werts relevanten Daten sind nicht an einem zentralen Ort gespeichert, sondern überall dort, wo die Blockchain selbst als Transaktionshistorie gespeichert ist. Vielmehr soll aber auch eine mehrfache und überörtliche Speicherung der betreffenden Einheiten eine elektronische Speicherung darstellen können.⁸²

[30] Zudem müsste der digitale Euro dazu genutzt werden, Zahlungsvorgänge im Sinne des § 675 f IV 1 BGB durchzuführen. Zahlungsvorgänge sind danach jede Bereitstellung, Übermittlung oder Abhebung eines Geldbetrags. Wird CBDC als E-Geld ausgestaltet, fällt sie mithin unter den Begriff des Geldbetrags und kann zur Durchführung von Zahlungsvorgängen genutzt werden. Die BaFin verleiht dem Begriff des Zahlungsvorgangs in Bezug auf E-Geld eine weitere Bedeutung und beschreibt ihn als Übertragung von monetären Werten.⁸³ Dies geht einher mit der Ansicht, das Regelungsobjekt des Geldbetrages beim E-Geld-Tatbestand auszulassen.⁸⁴ Sobald der digitale Euro ausgegeben wurde und er anstelle von Bar- oder Buchgeld als Zahlungsmittel von einem beliebigen Dritten für dessen Waren- oder Dienstleistungen akzeptiert wird, ist auch das Merkmal der Drittakzeptanz erfüllt. Mithin könnte CBDC durch-

aus als E-Geld ausgestaltet werden, zumal der E-Geld-Begriff gerade innovations- und entwicklungsorientiert konzipiert ist.⁸⁵

3. Abgrenzung zu privatem Blockchain-Geld am Beispiel von Libra

[31] Für Blockchain-basierte Zahlungsmittel, die nicht von hoheitlicher Stelle, sondern privat geschöpft werden, steht beispielhaft das von Facebook initiierte und von der Libra Association mit Sitz in Genf getragene Libra-Projekt. Libra funktioniert jedoch anders als herkömmliche Kryptowährungen wie Bitcoin oder Ether, deren Wert sich anhand von Angebot und Nachfrage bildet. Libra soll als Stable Coin an reale Währungen gekoppelt sein und somit einen konstanten Preis bilden.⁸⁶ Zielsetzung des Projekts ist die Schaffung einer einfachen, kostengünstigen und globalen Währung.⁸⁷ Mangels staatlicher Anerkennung und hoheitlichem Schöpfungsakt kann Libra keine Währung im währungsrechtlichen Sinne darstellen. Die privat emittierten „Kryptowährungen“ sollen gerade nicht zentral und staatlich gesteuert werden.⁸⁸ Eine Einordnung als Geld im Rechtssinne erscheint möglich. Den konkreten Geldbegriff erfüllt Libra zwar nicht. Eine Qualifizierung als Buch- oder E-Geld ist jedoch je nach konkreter Ausgestaltung nicht auszuschließen. Denn bei der Libra-Blockchain handelt es sich nicht um eine öffentliche Blockchain, sondern um eine "Consortium-Blockchain", in der jeder Partner des Konsortiums einen Netzwerkknoten betreiben soll.⁸⁹ Somit wird die Libra-Blockchain von diesen ausgewählten Mitgliedern verwaltet, die mithin auch den Libra-Token emittieren. Es besteht eine zentrale Instanz, bei der man auch eine Forderung geltend machen könnte. Libra kann damit grundsätzlich als E-Geld ausgestaltet werden.⁹⁰

V. Zahlungsdienstrecht

[32] Im Zusammenhang mit der Ausgabe und Nutzung von CBDC stellt sich die Frage, ob und inwieweit das

77 Vgl. BaFin, Hinweise zum ZAG, 29.11.2017, Ziff. 4. a) aa), abrufbar unter: <https://beck-link.de/w7tnv>.

78 Vgl. Auffenberg BKR 2019, 341 (343).

79 BeckOGK-BGB/Foerster (Stand: 15.6.2020), § 675 f Rn. 69.

80 So Maume/Maute/Wettlaufer/Patz, Rechtshandbuch Kryptowerte, 2020, § 13 Rn. 28 ff; a. A. BaFin (Fn. 78).

81 BaFin (Fn. 78).

82 Vgl. Auffenberg BKR 2019, 341 (343).

83 BaFin (Fn. 78).

84 Maume/Maute/Wettlaufer/Patz, Rechtshandbuch Kryptowerte, § 13 Rn. 32 f.

85 Vgl. Auffenberg BKR 2019, 341 (343).

86 Überblick bei Omlor, 3 Stanford Journal of Blockchain Law & Policy 83–95 (2020).

87 WhitePaper zu Libra (Stand 04/2020), abrufbar unter: <https://libra.org/de-DE/white-paper/>.

88 Omlor ZHR 183 (2019), 294 (307).

89 Brauneck WM 2019, 1911 (1914).

90 Maume/Maute/Wettlaufer/Patz, Rechtshandbuch Kryptowerte, § 13 Rn. 44 f.

Zahlungsdienstrecht der §§ 675 c ff. BGB Anwendungsfälle. Subsidiär kommt das allgemeine Geschäftsbesorgungsrecht nach § 675 I BGB in Betracht.

1. Anwendung der §§ 675 c ff. BGB

a) Persönlicher Anwendungsbereich

[33] Der persönliche Anwendungsbereich der §§ 675 c ff. BGB ist eröffnet, wenn im Zusammenhang mit der Ausgabe oder Verwaltung von CBDC ein Zahlungsdienstleister i. S. d. § 1 I 1 ZAG bzw. E-Geld Emittent i. S. d. § 1 II 1 ZAG in Erscheinung tritt. Da die EZB den digitalen Euro in hoheitlicher Funktion ausgeben würde, scheidet die Anwendung des ZAG im Verhältnis zwischen ihr und anderen Beteiligten aus.⁹¹ Eine Anwendung des Zahlungsdienstrechts kommt für das direkte Modell der Retail CBDC mithin nicht in Betracht. Beim hybriden und indirekten Modell von Retail CBDC sowie beim Modell der EZB können jedoch je nach Ausgestaltung die Intermediäre die Funktion als Zahlungsdienstleister bzw. E-Geld-Emittenten einnehmen.

b) Sachlicher Anwendungsbereich

[34] Der sachliche Anwendungsbereich der §§ 675 c ff. BGB setzt entweder einen Zahlungsdienst nach § 1 I 2 ZAG oder ein E-Geld-Geschäft nach § 1 II 2 ZAG voraus. Die Buchgeld- bzw. E-Geld-Eigenschaft von CBDC wird für diese Zwecke unterstellt, auch wenn die E-Geld-Einordnung von der konkreten Ausgestaltung abhängt.

aa) E-Geld-Geschäft

[35] E-Geld-Geschäft bedeutet die Ausgabe von E-Geld (§ 1 II 2 ZAG). Mit Ausgabe ist die Bereitstellung von geldwerten Einheiten bzw. die Übertragung von elektronischen Einheiten von der ausgebenden Stelle auf denjenigen, der sie zu Zahlungszwecken einsetzen will, gemeint.⁹² Beim hybriden Modell sowie beim EZB-Modell wird der digitale Euro von der EZB ausgegeben. Der Nutzer hält in jedem Fall selbst ein Konto bei der Zentralbank, das lediglich von einem Intermediär verwahrt bzw. verwaltet wird. Da die EZB den digitalen Euro jedoch in hoheitlicher Funktion ausgeben würde, kann hierbei kein E-Geld-Geschäft i. S. d. ZAG vorliegen. Zumindest beim indirekten Modell könnte jedoch eine Ausgabe von E-Geld als intermediäre CBDC stattfinden.

bb) Zahlungsdienst

[36] Zahlungsdienste sind alle in § 1 I 2 ZAG aufgezählten Dienste, beispielsweise Ein- und Auszah-

lungsgeschäfte oder die Ausführung von Zahlungsvorgängen in Hinblick auf die Führung eines Zahlungskontos. Beim Transfer von Buchgeld muss demnach jede Partei ein Zahlungskonto eingerichtet haben. Nach § 1 XVII ZAG ist ein Zahlungskonto ein auf den Namen eines oder mehrerer Zahlungsdienstnutzer lautendes Konto, das für die Ausführung von Zahlungsvorgängen genutzt wird. Es bestimmt die jeweilige Forderung gegen den Zahlungsdienstleister bzw. Zahlungsdienstnutzer und verbucht Zahlungsvorgänge.⁹³ Im Zusammenhang mit CBDC auf einer Blockchain ist fraglich, ob ein solches Zahlungskonto vorliegen kann. Da beim Transfer von CBDC Wallets zum Einsatz kommen, könnten diese als Zahlungskonten gelten. Das Wallet selbst speichert jedoch nicht den Euro-Token, der wiederum die Forderung gegen den Emittenten bestimmt, noch verbucht es Zahlungsvorgänge. Es speichert lediglich den privaten Schlüssel, durch den wiederum ein Token zugeordnet bzw. transferiert werden kann. Es wird gerade kein Wert an den Anbieter des Wallets transferiert, noch kann dieser über die jeweiligen Token verfügen. Wallets, die vom Nutzer selbst verwaltet werden, stellen demnach keine Zahlungskonten iSv § 1 XVII ZAG dar.⁹⁴ Zudem wäre der direkte Zugang zum Wallet nur beim direkten Modell vorstellbar, auf welches das ZAG jedoch von vornherein keine Anwendung findet.

[37] Der Wallet-Anbieter könnte jedoch als verwahrender Wallet-Anbieter fungieren und hätte damit alleinigen Zugang zum privaten Schlüssel des Nutzers. Durch den Zugriff auf den privaten Schlüssel können sie Transaktionen bezüglich der Euro-Token ausführen. Der Nutzer selbst könnte diese lediglich veranlassen. In diesem Zusammenhang wird erwogen, ob das Konto beim Wallet-Verwahrer aus Schutzzweckerwägungen als Zahlungskonto einzuordnen wäre.⁹⁵ Unter diesem Gesichtspunkt könnte auch der Transfer von Euro-Token, die als Buch- oder E-Geld ausgestaltet wären, als Zahlungsgeschäft i. S. d. § 1 I 2 Nr. 3 ZAG gelten. Die Einzahlung von Bargeld, das dem Nutzer in Form von Euro-Token „gutgeschrieben“ wird und über die er durch den privaten Schlüssel im Wallet verfügen bzw. Transaktionen zumindest veranlassen kann, ist dann ebenfalls als Zahlungsdienstleistung anzusehen. Dasselbe gilt für die Ausgabe von CBDC durch Kreditvergabe. Diese Konstellation wäre beim hybriden Modell und beim EZB-Modell möglich, jedoch nur, wenn das Wallet von einem Intermediär und nicht von der EZB selbst angeboten wird. Da die EZB kein konto-

⁹¹ Siehe oben, sub V. b. (2) E-Geld.

⁹² Casper/Terlau/Terlau, ZAG, § 1 Rn. 239.

⁹³ Casper/Terlau/Casper, ZAG § 1 Rn. 35.

⁹⁴ So auch Maume/Maute/Wettlaufer/Patz, Rechtshandbuch Kryptowerte, § 13 Rn. 64.

⁹⁵ Maume/Maute/Wettlaufer/Patz, Rechtshandbuch Kryptowerte, § 13 Rn. 68 f.

führender Zahlungsdienstleister sein kann, könnte ein solches Wallet auch nicht als Zahlungskonto i. S. d. ZAG gelten.

[38] Es besteht jedoch die Möglichkeit, das Wallet bei der EZB mit einem herkömmlichen Zahlungskonto bei einem Intermediär zu verknüpfen. Über dieses könnte der Handel mit der CBDC bezahlt werden.⁹⁶ Das Zahlungsdienstrecht wäre in der Konsequenz zwischen Intermediär und Nutzer anwendbar. Dies wäre beim hybriden Modell und beim EZB-Modell vorstellbar. Beim indirekten Modell verfügt der Nutzer selbst über kein Konto bzw. Wallet bei der EZB. Die Endkunden halten ein Konto direkt beim Intermediär, über dieses sie lediglich Zugriff auf die „intermediäre“ CBDC haben. Dieses kann je nach Form der „intermediären“ CBDC als klassisches Girokonto oder E-Geld-Konto ausgestaltet sein und somit die Voraussetzungen eines Zahlungskonto i. S. d. ZAG erfüllen. Auch hier könnte das Zahlungsdienstrecht zwischen Intermediär und Nutzer anwendbar sein.

[39] Des Weiteren könnte das Blockchain-Netzwerk selbst als Zahlungskonto i. S. d. ZAG fungieren. Die jeweilige Blockchain dient der Erfassung von Token-Transaktionen, die der Verbuchung von Zahlungsvorgängen ähnlich ist.⁹⁷ Eine Blockchain kann damit grundsätzlich Forderungen zwischen den Nutzern des digitalen Euro und der EZB darstellen. Fraglich hierbei ist jedoch, wer in diesem Fall der kontoführende Zahlungsdienstleister i. S. v. § 1 XVIII ZAG wäre. Die EZB fällt aus dem Anwendungsbereich des ZAG. Wird die Blockchain durch einen externen Anbieter betrieben, stellt dieser in der Regel keinen Zahlungsdienstleister dar, da sich keine Forderungen der Nutzer gegen ihn richten.⁹⁸

2. Allgemeines Geschäftsbesorgungsrecht

[40] Sind die §§ 675c ff. BGB nicht anwendbar, kann auf die Vorschriften des allgemeinen Geschäftsbesorgungsrechts zurückgegriffen werden. Da davon auszugehen ist, dass die Kontoführung bei der Zentralbank unabhängig vom gewählten Modell nicht kostenfrei ausgestaltet sein wird, ist über eine entgeltliche Geschäftsbesorgung nach § 675 BGB nachzudenken. Danach sind auf einen Dienstvertrag oder einen Werkver-

trag, der eine Geschäftsbesorgung zum Gegenstand hat, ausgewählte Vorschriften des Auftragsrechts anzuwenden. Entgeltliche Geschäftsbesorgung i. S. v. § 675 BGB bedeutet, dass der Geschäftsbesorger gegenüber dem Geschäftsherrn dazu verpflichtet ist, eine selbstständige Tätigkeit wirtschaftlicher Art zur Wahrnehmung fremder Vermögensinteressen auszuführen.⁹⁹ Diese Definition lässt sich auch auf die Leistung, die die Zentralbank anbieten könnte, übertragen, die dann als Geschäftsbesorgerin anzusehen wäre. Die Kunden halten Konten bzw. Wallets direkt bei der Zentralbank, die entweder von ihr selbst oder Intermediären verwaltet werden. Der Kunde kauft beispielsweise über Bargeld Euro-Token ein und die Zentralbank schreibt diese dessen Konto bzw. Wallet zu.¹⁰⁰

VII. Zusammenfassung

1. Es besteht ein praktischer Bedarf an CBDC, der sich vor allem aus der effizienten Abwicklung des (internationalen) Zahlungsverkehrs und dem Einsatz von automatisierten Prozessen ergibt.
2. Primärrechtlich ist die Einführung von CBDC ohne Vertragsänderung möglich; das Sekundärrecht in Gestalt vor allem der EuroEinfVO müsste hingegen angepasst werden.
3. Der digitale Euro kann als gesetzliches Zahlungsmittel und damit zugleich als Geld im Rechtssinne etabliert werden.
4. Die Regulierung von CBDC fällt nur unter das ZAG und das BGB-Zahlungsdienstrecht, soweit nicht die EZB als Währungsbehörde unmittelbar die Ausgabe vornimmt, sondern sich für die Rechtsbeziehung zu den Nutzern Intermediären (z. B. Geschäftsbanken) bedient.
5. Der digitale Euro kann als E-Geld ausgestaltet werden. Zahlungsdienste mit CBDC liegen indes *de lege lata* nur vor, wenn ein Zahlungskonto i. S. d. § 1 XVII ZAG verwendet wird.

⁹⁶ Vgl. Maume/Maute/Wettlaufer/Patz, Rechtshandbuch Kryptowerte, § 13 Rn. 67.

⁹⁷ Vgl. Keding WM 2018, 64 (68 f.).

⁹⁸ Vgl. Keding WM 2018, 64 (69).

⁹⁹ BGH NJW 1966, 1452; NJW 1989, 1216 (1217); NJW-RR 1992, 560; NJW-RR 2004, 989.

¹⁰⁰ Vgl. Kirschbaum/Stepanova BKR 2019, 286 (288).

RA Dr. Thorsten Voß*

Lessons to be learned?

Zur causa Wirecard und der aufsichtsrechtlichen Regulierung von FinTechs

Ein Kriminalfall noch nie dagewesenen Ausmaßes erschüttert im Sommer 2020 Anleger, Marktteilnehmer, Wirtschaftsprüfer, Behörden und die Politik: Ein Schurkenstück führte einen FinTech-Anbieter von Dienstleistungen rund um die Glücksspiel- und Pornobranche durch augenscheinlich manipulierte Bilanzen und Luftbuchungen bis hinauf in den DAX, dann krachend in die Insolvenz. Der erwartbare Antrag auf Einsetzung eines Parlamentarischen Untersuchungsausschusses liest sich, als hätte John le Carré die Feder geführt und möchte nicht nur ein etwaiges Versagen der Finanzaufsicht, sondern gar etwa auch die Rolle der Geheimdienste klären. Eine Verfilmung ist in Vorbereitung. Es stellt sich die Frage, ob und wie behördenseitig früher hätte erkannt werden können, welches Spiel hier am Kapitalmarkt getrieben wurde, und ob infolgedessen ein Reformbedarf der gesetzlichen Grundlagen besteht. Der folgende Beitrag unterzieht das – wohl unbestritten – engmaschige Netz, durch das die Wirecard AG geschlüpft ist, einer insbesondere rechtspolitischen Würdigung und gibt Empfehlungen für eine Verbesserung der aufsichtsrechtlichen Regulierung von FinTechs.

I. Einleitung

„Wir fühlen uns zuständig, sind wir es nicht, klären wir die Zuständigkeit aktiv.“

„Wir sind bereit, Fehler zuzugeben und uns zu entschuldigen.“

„Das, was gut ist, wertschätzen, an dem, was nicht gut ist, arbeiten.“

Aus: Wertekanon für den Umgang und die Zusammenarbeit in der BaFin (Stand: 2015)

[1] Wenn FinTechs¹ bisher über eines nicht klagen konnten, dann darüber, dass sie die vernachlässigten Kinder des deutschen Kapitalmarkt- und des Aufsichtsrechts waren. „Ich bin kein Sandbox-Präsident!“ ließ sich BaFin-Präsident Felix Hufeld noch auf der BaFin-Tech 2019 vernehmen und in der Tat – wer als FinTech einen Zulassungstatbestand im Aufsichtsrecht auslöst, goes for the full monty und muss wie ein jeder Finanzdienstleister und jede Wertpapierfirma „das volle Pflichtenprogramm“ erfüllen, um am Kapitalmarkt tätig werden zu können.² Sonderzonen, wie sie etwa dem angelsächsischen Rechtskreis bekannt sind und in dem FinTechs sich erproben und erste Erfahrungen mit einem „Regulierungsrahmen light“ machen können³, sind der

deutschen Aufsichtsrechtsordnung unbekannt. Gleichwohl hat dies von der Zeit vom FinTech⁴ bis zum Aufstieg in den maßgeblichen deutschen Aktienindex DAX die Akteure der Wirecard AG jedenfalls nicht daran zu

* Rechtsanwalt und Partner der Sozietät Schalast & Partner in Frankfurt am Main, Bankkaufmann, Lehrbeauftragter an der Frankfurt School of Finance & Management und Dozent im Fachanwaltslehrgang für Bank- und Kapitalmarktrecht. Sämtliche Internetquellen wurden zuletzt am 5.11.2020 abgerufen.

1 Vgl. zum Begriff statt aller Möslein/Omlor/diess., FinTech-Handbuch, 2019, § 1 Rn. 1 ff.

2 Selbstredend kann dabei auf Gestaltungsmöglichkeiten wie sog. *Fronting*-Lösungen zurückgegriffen werden, was insbesondere bei Kreditplattformen und Zahlungsdienstleistungen von Belang ist; die BaFin weist in ihren einschlägigen Merkblättern selbst darauf hin.

3 Zu *Sandbox*-Ansätzen instruktiv Möslein/Omlor/Chiu, FinTech-Handbuch, § 22.

4 Die Muttergesellschaft Wirecard AG war im Verhältnis zu ihrer Tochtergesellschaft Wirecard Bank AG als Zahlungsabwickler ein nahezu paradigmatisch typisches „FinTech“, was als Technologieunternehmen gleichwohl nicht als Finanzholding eingestuft und als „Nicht-Bank“ betrachtet wurde. Als solches qualifizierte es sich zwar für die allgemeine Marktaufsicht, der sämtliche börsennotierte Unternehmen unterstehen, fiel aber im Übrigen nicht unter zahlreiche Aufsichtskompetenzen der BaFin, namentlich im Bereich der Geldwäsche gem. § 51 KWG. Gem. § 50 Nr. 9 GwG liegt nun in den verbleibenden Konstellationen, in denen ein Unternehmen als Verpflichteter nach dem GWG anzusehen ist, die Zuständigkeit für die Geldwäscheaufsicht bei den nach Landesrecht zuständigen Stellen. Dies war hier die Bezirksregierung von Niederbayern, die am 25.2.2020 erstmals mit der BaFin Kontakt aufnahm und mitteilte, dass sie sich als zuständige Geldwäscheaufsichtsbehörde über die Wirecard AG ansieht. Dies mag unfreiwillig komisch, wenn nicht gar grotesk wirken, ist aber nichts anderes als die Konsequenz der durch die Legislative vorgegebenen Regeln – Vgl. zur Geschäftstätigkeit der Wirecard AG insgesamt unten Fn. 13.

hindern vermocht, ihre – offenbar mit zuvor kaum vorstellbarer krimineller Energie – betriebene Täuschungsmaschine ins Werk zu setzen, welche einen Schaden in Milliardenhöhe in den Taschen der Anleger und mehr als nur eine enorme Reputationsdelle für den Finanzplatz Deutschland verursachte. Im Sommer 2020 klingt der BaFin-Präsident denn auch ganz anders: „*Ich würde mir wirksamere Möglichkeiten für uns wünschen*“⁵, so heißt es nun.⁶ Der Gesetzgeber agierte zeitnah und legte bereits am 26. Oktober 2020 den Entwurf eines Gesetzes zur Stärkung der Finanzmarktintegrität („FISG“)⁷ vor, den es auch in diesem Beitrag zu reflektieren gilt.

[2] Dabei ist der Wirecard-Skandal wohl ein solcher genau zur richtigen Zeit, koinzidiert er doch nicht nur mit dem *Brexit*, sondern auch mit der deutschen EU-Ratspräsidentschaft und damit in einer Periode besonderer Verantwortung für die Regulierung von Marktakteuren.⁸ Was ist aufsichtsrechtlich zu tun? Zunächst sind die verschiedenen Akteure auseinander zu halten. Der *cast of characters* in der *causa* Wirecard stellt so unterschiedliche Institutionen wie die Finanzaufsicht BaFin, die DPR, die mandatierte Wirtschaftsprüfungsgesellschaft, aber auch die Deutsche Börse AG und den Aufsichtsrat der Wirecard AG an den Pranger. Und da bei einem so großen Schadensfall ein Systemversagen und ein nicht funktionierendes Ineinandergreifen der vorgenannten Institutionen in Rede steht, gehören auch alle genannten Einheiten und ihre Wirkweisen auf den Prüfstand. Einen etwaigen Regulierungsbedarf für alle diese Teilnehmer auszuloten, würde indessen den Rahmen dieses Beitrags sprengen und muss weiteren Folgeuntersuchungen vorbehalten bleiben, kommen hier doch ganz unterschiedliche Paradigmen zum Tragen. So ist die Rolle der Wirtschaftsprüfer etwa maßgeblich von dem von Rating-Agenturen bekannten *capture* Problem geprägt, zahlt für die Prüfung doch das Unternehmen und nicht die öffentliche Hand, was im Wettbewerb um die Mandatsgewinnung und den -erhalt zu sachfremden Erwägungen und Praktiken führen mag – dies ist ein Diskussionsstrang für sich.⁹

[3] Hier sei indessen die Finanzaufsicht als der neben den Wirtschaftsprüfern womöglich reizvollste Akteur in den Fokus genommen. Auch wenn die Ergebnisse des Parlamentarischen Untersuchungsausschusses („PUA“)¹⁰ noch nicht vorliegen und der Sachverhalt für Außenstehende daher nicht nach einer feststehenden Aktenlage beurteilt werden kann, sind doch gewisse Analysen und Schlussfolgerungen möglich. So findet sich ein verdienstvoller und in der öffentlichen Diskussion viel zu wenig beachteter Sachstandsbericht zur Chronologie der Ereignisse auf der Website des BMF.¹¹ Auch die ESMA hat die Ergebnisse einer sog. *Fast Track Peer Review*, der ersten dieser Art nach der neuen ESMA-VO, nunmehr am 3. November 2020 veröffentlicht und unterzieht dort die Ereignisse, die zum Zusammenbruch

der Wirecard AG führten, und das aufsichtsrechtliche Agieren der BaFin der DPR einer Bewertung.¹² Aus diesen Dokumenten erhellt – ungeachtet der kritischen Äußerungen an der Arbeit der involvierten Institutionen – jeweils, dass die BaFin vielfach mit dem ihr zur Verfügung stehenden Instrumentarium tätig geworden ist. Warum dann dieser Schaden? Soll der Fall Wirecard Anlass für eine Neujustierung bestehender Regulierung dienen, sind die aus diesem Fall, in seinen extremen Ausprägungen nahezu eine *caricature of fraud*, verallgemeinerungsfähigen Defizite herauszuarbeiten, so sie denn überhaupt bestehen sollten.¹³

[4] Zu beachten ist, dass der Fall Wirecard exemplarisch die Unterschiede in der Aufsichtskultur einer Instituts- und Marktaufsicht verdeutlichen mag.¹⁴ Dem

5 Vgl. DIE ZEIT, Interview mit Felix Hufeld vom 2.7.2020, abrufbar unter: <https://beck-link.de/ec6ka>.

6 Ein Aktionsplan wurde durch das BMF denn auch zügig zur Verfügung gestellt, wonach die Kontroll- und Zugriffsrechte der BaFin insbesondere im Hinblick auf Bilanzmanipulationen hochgezäumt werden sollen; vgl. RP Online, Olaf Scolz freut sich auf den Wirecard-Untersuchungsausschuss, 7.10.2020, abrufbar unter: <https://beck-link.de/6ynfx>.

7 Im Internet abrufbar unter: <https://beck-link.de/8an3p>. Neben einer Reform des zweistufigen Enforcementverfahrens enthält das FISG-E auch – in diesem Beitrag nicht zu behandelnde – Maßnahmen zur Stärkung der Unabhängigkeit der Abschlussprüfer, indem auch für Kapitalmarktunternehmen fortan eine verpflichtende externe Prüferrotation nach zehn Jahren vorgesehen ist und indem die Pflicht zur Trennung von Prüfung und Beratung bei Unternehmen von öffentlichem Interesse wesentlich ausgeweitet wird. Zudem wird die zivilrechtliche Haftung des Abschlussprüfers gegenüber dem geprüften Unternehmen für Pflichtverletzungen verschärft; durch Anpassungen im Bilanzstrafrecht soll eine ausreichend abschreckende Ahndung der Unternehmensverantwortlichen bei Abgabe eines unrichtigen „Bilanz-eids“ und der Abschlussprüfer bei Erteilung eines inhaltlich unrichtigen Bestätigungsvermerks zu Abschlüssen von Unternehmen von öffentlichem Interesse ermöglicht werden. Weiter werden im Bilanzordnungswidrigkeitenrecht insb. die Bußgeldvorschriften für Abschlussprüfer, die Unternehmen von öffentlichem Interesse prüfen, inhaltlich ausgeweitet und der Bußgeldrahmen erfährt eine deutliche Anhebung.

8 So auch *Langenbucher* EuZW 2020, 681.

9 Angedacht etwa bei *Langenbucher* EuZW 2020, 681 (682), die *joint audits* als ein mögliches Gegenmittel ins Feld führt.

10 Es bedarf im Übrigen keines überdimensionierten Vorstellungsvermögens zu imaginieren, dass die Behörde in den Tagen der Schlussredaktion dieses Beitrags mit der Bearbeitung von Wirecard-spezifischen Eingaben sowie der Zusammenstellung von Unterlagen für den PUA – schon zur Einhaltung des Datenschutzes – in weiten Teilen für die Fachaufsicht „lahmgelegt“ sein dürfte. Kohorten von Sachbearbeitern dürften derzeit Akten schwärzen, statt neue aufzumachen – ein Trauerspiel für sich, über das nicht gefrotzelt sein soll.

11 Vgl. Bundesministerium der Finanzen, Sachstandsbericht und Chronologie Wirecard, 16.7.2020, abrufbar unter: <https://beck-link.de/wh4vc>.

12 ESMA, Fast track peer review on the application of the guidelines on the enforcement of financial information (ESMA/2014/1293) by BaFin and FREP in the context of Wirecard, 3.11.2020, abrufbar unter: <https://beck-link.de/6pznf>.

13 Vgl. zu verhaltensökonomischen und kognitionswissenschaftlichen Erkenntnissen in diesem Kontext *Langenbucher* ZGR 2019, 717.

14 Im Einzelnen besteht bzw. bestand der Wirecard-Konzern aus zahlreichen – meist global agierenden – Gesellschaften mit der Wirecard AG mit Sitz in Deutschland an der Spitze. Der Konzern nutzte innerhalb Europas im Wege des Europäischen Passes die von der BaFin direkt beaufsichtigte Wirecard Bank AG und die von der britischen Finanzaufsicht FCA beaufsichtigte Wirecard Card Solutions Limited für sein aufsichtsunterworfenen Geschäft (insb. Zahlungsdienst-Geschäft, E-Geld-Geschäft). Außerhalb Europas verfüg(t)en konzernangehörige Gesellschaften der Wirecard AG in einigen Ländern über eigene (E-Geld) Lizenzen vor Ort (z. B. Philippinen, Singapur). In anderen Ländern arbeiten sie als finanztechnologische Dienstleister mit lokalen –

Verf. sind noch sehr gut die Worte von ED WA aD Georg Dreyling im Ohr, der ihm gegenüber einst sinn gemäß feststellte: „In Bonn, da ist die Institutsaufsicht, das sind die Beiboote, die gemächlich neben den Tankern rudern und ab und zu entern, um zu schauen, ob an Bord alles in Ordnung ist. Wir in Frankfurt sind aber die Schnellboote, die auf dem Fluss kreisen, und wo sich wie ein Fisch ein Marktverstoß zeigt, da rammen wir unsere Speere hinein“. Dies lässt sich nicht nur auf ein gefälliges *bon mot* reduzieren, sondern weist auf ein Grundthema der Marktaufsicht hin: Verstöße gegen eine Vielzahl von wertpapierhandelsrechtlichen Vorschriften werden von einzelnen Schnellbooten verfolgt, was heißt das aber *for the big picture*?

[5] Vor diesem Hintergrund rücken die folgenden Instrumente bzw. Fragenkreise in den Blick, die der Beitrag skizziert: die Bilanzkontrolle (II.), Marktmanipulation und Leerverkaufsverbote (III.) sowie die Generalklausel des § 6 WpHG (IV.), bevor ein Fazit für Perspektiven der aufsichtsrechtlichen Regulierung von FinTechs unter Würdigung des FISG (V.) zu ziehen ist.

II. Die Bilanzkontrolle

[6] Es sei zunächst das System der Bilanzkontrolle im deutschen Wertpapierhandelsrecht in Erinnerung rufen, das, da es ja augenscheinlich um offensichtlich gefälschte Unternehmensabschlüsse geht, ganz besonders in den Fokus des Interesses rückt. Nicht wenige Anleger zeigten sich überrascht, als sie von der Zweistufigkeit des deutschen Enforcementverfahrens (erst) im Zuge der Wirecard-Affäre erfuhren und äußerten sich – auch gegenüber dem *Verf.* – durchaus mit mokantem Unterton, was denn „da alles ans Licht kam“. Nun, ans Licht kam nichts, waren das Verfahren und das Zusammenspiel zwischen BaFin und DPR doch seit Jahr und Tag auf der Website der BaFin dargestellt.¹⁵ Bezogen auf die Bilanzkontrolle sind nun Fragen bezüglich des Verhältnisses zwischen der DPR (§§ 342 b ff. HGB) und der BaFin (§§ 106 ff. WpHG) und damit zwischen der ersten und zweiten Stufe des gegenwärtigen Enforcementverfahrens aufgeworfen. Es mag sich insbesondere die Frage stellen, ob die BaFin bei im Raum stehenden Betrugshandlungen eines Emittenten die Durchführung des Enforcementverfahrens von der DPR an sich ziehen bzw. unmittelbar selbst durchführen kann, aber nicht nur: Fraglich ist auch, wie das Verfahren zur Bekämpfung von Bilanzmanipulation und die Befugnisse zur Bekämpfung von Marktmanipulation sich im Aufsichtsrecht zueinander verhalten. Bilanzmanipulation ist ersichtlich eine der denkbar schwersten Formen von Marktmanipulation. Sperrt etwa ein laufendes Enforcementverfahren ein Tätigwerden aufgrund marktmanipulationsrechtlicher Befugnisse?

1. Institutionen der Bilanzkontrolle

[7] Zunächst sei daran erinnert: Das deutsche Enforcementverfahren ist ein Kind des BilKoG. Nach der Begründung des Regierungsentwurfs soll das BilKoG das Vertrauen der Anleger in den Kapitalmarkt wiederherstellen und weiter stärken¹⁶, das Gegenteil ist mit der *causa* Wirecard nun der Fall. Ziel war es, Unregelmäßigkeiten bei der Erstellung von Unternehmensabschlüssen und -berichten präventiv entgegenzuwirken und, sofern Unregelmäßigkeiten dennoch auftreten, diese aufzudecken und den Kapitalmarkt darüber zu informieren.¹⁷ Weiterhin ging der seinerzeitige Gesetzgeber explizit davon aus, dass neben dem bestehenden System zur Durchsetzung der Rechnungslegungsvorschriften durch Prüfung der Jahres- und Konzernabschlüsse durch den Abschlussprüfer und Aufsichtsrat, den aktienrechtlichen Vorschriften zur Nichtigkeit von Jahresabschlüssen sowie Straf- und Sanktionsvorschriften, ein von staatlicher Seite beauftragtes Gremium, neben Abschlussprüfer und Aufsichtsrat,¹⁸ erforderlich ist, um regelmäßig die Richtigkeit der Unternehmensberichte kapitalmarktorientierter Unternehmen zu prüfen.¹⁹ Hierdurch sollte das Enforcementverfahren ergänzend und subsidiär zu den bereits zum Zeitpunkt des Inkrafttretens des BilKoG bestehenden gesellschafts- und bilanzrechtlichen Kontrollmechanismen mit dem erklärten Ziel, Bilanzmanipulationen zu verhindern, ausgestaltet werden²⁰.

soweit bekannt – jeweils der lokalen Finanzaufsicht unterworfenen – Partnern zusammen, ohne über eine eigene Lizenz zu verfügen. Als Konzernmutter übte die Wirecard AG selbst keine operative Geschäftstätigkeit in den fraglichen Bereichen aus. Daher erbrachte sie keine Bank- oder Zahlungsdienstleistungen iSd Aufsichtsgesetze, daher wurde sie nicht von der BaFin als Kreditinstitut, Zahlungsinstitut oder E-Geld Institut beaufsichtigt. Die Frage, ob ein Unternehmen als Finanzholding eingeordnet wird, beantwortet sich nach Art. 4 I 1 Nr. 20 CRR. Hiernach erfolgt eine Einstufung eines Unternehmens als Finanzholding, wenn dessen Tochterunternehmen ausschließlich oder hauptsächlich Institute oder Finanzinstitute sind. Nach gemeinsamer Prüfung durch Deutsche Bundesbank und BaFin im Jahre 2017 und in Übereinstimmung mit einer späteren Bestätigung durch die EZB – es waren also drei (*sic!*) Institutionen an dieser Entscheidungsfindung beteiligt – war die Wirecard AG aufgrund des Schwerpunkts ihrer Tätigkeit und der ihrer Tochtergesellschaften keine Finanzholding mit der Folge, dass lediglich die Wirecard Bank AG unter der Aufsicht der BaFin stand; vgl. im Einzelnen den Sachstandsbericht des BMF (Fn. 11).

¹⁵ Vgl. jetzt etwa den einschlägigen Auszug aus dem Emittentenleitfaden, abrufbar unter: <https://beck-link.de/d5nsv>.

¹⁶ Entwurf eines Gesetzes zur Kontrolle von Unternehmensabschlüssen (Bilanzkontrollgesetz – BilKoG), BT-Drucks. 15/3421, S. 11.

¹⁷ Ebd.

¹⁸ Vgl. zum Zusammenspiel dieser Institutionen Klöhn/Mock/*ders.*, FS 25 Jahre WpHG, 2019, S.1064 ff.

¹⁹ Entwurf eines Gesetzes zur Kontrolle von Unternehmensabschlüssen (Bilanzkontrollgesetz – BilKoG), BT-Drucks. 15/3421, S. 11.

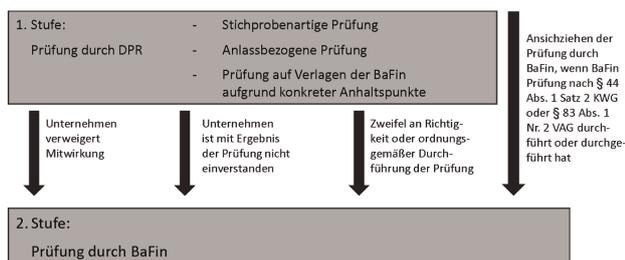
²⁰ Fuchs/Zimmermann WpHG, 2. Aufl. 2016, § 37 n Rn. 11; Just/Voß/Ritz/Becker/Labudda, WpHG, 1. Aufl. 2015, § 37 n Rn. 6. Nach diesem System erfolgt die Bilanzkontrolle nach der Bilanzaufstellung durch den Vorstand zunächst extern durch den Abschlussprüfer im Rahmen der gesetzlichen Abschlussprüfung (§§ 316 ff. HGB). Sollte es bei der Abschlussprüfung keine Einwände geben, erteilt der Abschlussprüfer den Bestätigungsvermerk (§ 322 HGB). Danach sind die Abschlüsse gesellschaftsintern durch den Aufsichtsrat zu prüfen (§ 171 AktG). Mit Billigung des Jahresabschlusses ist dieser festgestellt (§ 173 AktG). Gegebenenfalls haben die Aktionäre die Möglichkeit, eine

[8] Für kapitalmarktorientierte Unternehmen erfolgt eine Bilanzkontrolle im Ergebnis damit durch nicht weniger als die vier Institutionen (1) Abschlussprüfer, (2) Aufsichtsrat, (3) ggf. gerichtliches Kontrollverfahren und (4) Enforcementverfahren nach §§ 106 ff. WpHG, §§ 342 b ff. HGB.

2. Zweistufiger Verfahrensaufbau

[9] Das Enforcementverfahren selbst hat einen zweistufigen Aufbau, der ausweislich der Gesetzesbegründung gesetzgeberseitig so gewünscht war.²¹ Sofern eine privatrechtlich organisierte Prüfstelle gemäß § 342 b I 1 HGB anerkannt ist, obliegt zunächst dieser die Prüfung der Rechnungslegung kapitalmarktorientierter Unternehmen (§ 342 b II 1 HGB, § 108 I WpHG). Bis zur Anerkennung der DPR durch das BMJ, im Einvernehmen mit dem BMF mit Wirkung zum 30.3.2005²² auf Grundlage des § 342 b I 1 HGB, gab es lediglich ein einstufiges System der Überwachung und Durchsetzung ordnungsgemäßer Rechnungslegung durch die BaFin. Die Mitwirkung der dem Enforcementverfahren unterliegenden Unternehmen kann auf der ersten Stufe nicht von der DPR erzwungen werden, so dass die DPR – misslicherweise – bei ihren Prüfungen auf die Kooperation der Unternehmen angewiesen ist; vgl. § 342 b IV 1 HGB. Ursprünglich hatte man dies als Stärke des Verfahrens angesehen, würden die betroffenen Unternehmen doch so besser mitwirken. Mit Anerkennung der DPR ist die BaFin erst auf der zweiten Stufe für die Rechnungslegungsprüfung zuständig. Die BaFin greift nach Maßgabe des § 108 I 2 WpHG erst ein, wenn (1) ein Unternehmen seine Mitwirkung verweigert oder nicht mit dem Ergebnis der Prüfung einverstanden ist (§ 108 I 2 Nr. 1 WpHG), (2) erhebliche Zweifel an der Richtigkeit des Prüfungsergebnisses der Prüfstelle oder an der ordnungsgemäßen Durchführung der Prüfung durch die Prüfstelle bestehen (§ 108 I 2 Nr. 2 WpHG). Darüber hinaus kann die BaFin die Prüfung jederzeit gem. § 108 I 4 WpHG an sich ziehen, wenn sie auch eine Prüfung nach § 44 I 2 KWG oder § 83 I Nr. 2 des VAG durchführt oder durchgeführt hat und die Prüfung denselben Gegenstand betrifft²³ – jüngst ist dies im Fall der Grenke Leasing AG geschehen.²⁴

[10] Einen Überblick über die grundsätzliche Systematik des zweistufigen Verfahrensaufbaus gibt die nachstehende Abbildung:²⁵



[11] Dem zweistufigen Verfahren folgend verteilen sich die Bestimmungen des BilKoG auf zwei Gesetze. Soweit die erste Stufe des Verfahrens und damit die DPR betroffen ist, finden sich die einschlägigen Bestimmungen in den §§ 342 b bis 342 e HGB. Die Bestimmungen, die bei Tätigwerden der BaFin einschlägig sind, finden sich in §§ 106 bis 113 WpHG. Nach dem Wortlaut von § 106 WpHG obliegt es der BaFin, die Ordnungsmäßigkeit der Rechnungslegung kapitalmarktorientierter Unternehmen zu prüfen. Hintergrund dafür ist, dass bei Verabschiedung des BilKoG noch nicht feststand, ob eine private Prüfstelle gem. § 342 b HGB eingerichtet und anerkannt werden würde. Die §§ 106 und 107 WpHG normieren aus diesem Grund die Aufgaben und Befugnisse der BaFin im Bereich der Bilanzkontrolle umfänglich, so dass eine Prüfung der Rechnungslegung für den Fall, dass eine private Prüfstelle nicht eingerichtet und anerkannt worden wäre, auch im Wege eines einstufigen Verfahrens gewährleistet gewesen wäre. In diesem Fall hätte die BaFin die Kontrolle der Rechnungslegung in allen Fällen selbst durchführen müssen. Diese Aufgabe ist, wie in § 106 sowie § 108 I WpHG zum Ausdruck kommt, der BaFin allerdings nur „vorbeholdlich § 342 b II 3 Nr. 1 und 3 des Handelsgesetzbuchs“ zugewiesen. § 108 I WpHG schränkt die Befugnisse der BaFin nach § 107 WpHG zur Anordnung einer Prüfung der Rechnungslegung und ihre Ermittlungsbefugnisse stark ein, sofern eine Prüfstelle anerkannt ist. Da die DPR auf Grundlage von § 342 b I 1 HGB mit Wirkung vom 30. März 2005 anerkannt worden ist, ist die BaFin erst auf der zweiten Stufe bei der Bilanzkontrolle involviert – wie dies auch bei der Wirecard AG der Fall war.

[12] Hier informierte die BaFin im Rahmen des zweistufigen Verfahrens am 14. Februar 2019 das BMF, dass sie die Prüfung des verkürzten Abschlusses der Wirecard zum 30. Juni 2018 einschließlich des Lageberichts von der DPR verlangen wird und wegen mutmaßlicher Marktmanipulation in alle Richtungen, d. h. auch gegen die Wirecard AG, untersucht. Nur einen Tag später, am 15. Februar 2019, verlangte die BaFin die

Korrektur im Wege eines gerichtlichen Kontrollverfahrens in Gestalt der Nichtigkeitsklage gem. § 257 AktG oder einer Sonderprüfung wegen Unterbewertung gem. § 258 ff. AktG zu erzwingen. Dabei entfallen Nichtigkeitsklage und Sonderprüfung gemäß § 107 II und § 342 b III HGB eine Sperrwirkung gegenüber dem Enforcementverfahren. Die §§ 106 ff. und §§ 342 b ff. HGB stellen neben den vorhandenen gesellschafts- und bilanzrechtlichen Regelungen in der Sache daher eine weitere Kontrollinstanz dar. Vgl. für Details Assmann/Schneider/Mülbart/Hönsch, WpHG, 7. Aufl. 2019, Vor § 106 Rn. 4 ff.

21 Entwurf eines Gesetzes zur Kontrolle von Unternehmensabschlüssen (Bilanzkontrollgesetz – BilKoG), BT-Drucks. 15/3421, S. 11.
 22 Anerkennungsvertrag, im Internet abrufbar unter www.frep.info.
 23 Just/Voß/Ritz/Becker/Labudda, WpHG, § 37 n Rn. 10.
 24 Bei der Wirecard AG standen solche Prüfungen überhaupt nicht im Raum, wurde sie doch überhaupt nicht vom persönlichen Anwendungsbereich der Normen des KWG und VAG erfasst.
 25 Nach Just/Voß/Ritz/Becker/Labudda, WpHG, § 37 n Rn. 11.

Prüfung des verkürzten Abschlusses 2018 von der DPR – in der Sache eine Prüfung der Rechnungslegung der Wirecard AG auf Verlangen der BaFin gem. §§ 108 II, 107 I 1 WpHG. Am 15. April 2019 setzte die BaFin dann wegen früherer Verstöße gegen Finanzberichterstattungsvorschriften (teilweise verspätete Veröffentlichung des Halbjahresfinanzberichts für das Geschäftsjahr 2018, verspätete Veröffentlichung der Hinweisbekanntmachung) ein Bußgeld gegen die Wirecard AG iHv 1,52 Mio. Euro fest. Die Wirecard AG akzeptierte das Bußgeld iHv 1,52 Mio. Euro wegen Verstößen gegen Finanzberichterstattungspflichten nach § 115 WpHG, ging allerdings gegen die Veröffentlichung dieser Maßnahme vor, die nach entsprechender Entscheidung des HessVGH im September 2019 gleichwohl konsequent vorgenommen wurde. Zudem wurde in den Quartalsgesprächen der BaFin mit der DPR stets das Thema „Wirecard-Prüfung“ besprochen. Weiter erstattete die BaFin am 1. November 2019 an das BMF einen Bericht zum Wirecard-Marktmanipulationsverfahren und DPR-Untersuchungen und wies auf die begonnene forensische Sonderprüfung durch die KPMG hin. Am 30. April 2020 verlangte die BaFin von der DPR die Prüfung des Konzernabschlusses zum 31. Dezember 2018.²⁶ Schließlich erfolgte am 15. Mai 2020 ein BaFin-Bericht an das BMF über Stand der DPR-Prüfung des verkürzten Abschlusses zum 30.6.2018 mit der Ankündigung der DPR, das Prüfungsergebnis ggf. im Juli 2020 vorzulegen.²⁷

[13] Legt man nun zugrunde, dass Rechnungslegungsrecht stets Marktinformationsrecht ist, da eine zentrale Aufgabe jeder Bilanz in allen Regelungsbereichen die Vermittlung von Informationen an den jeweiligen Adressaten ist²⁸, so war nicht nur der Prozess des zweistufigen Verfahrensaufbaus insgesamt ersichtlich objektiv zu langsam, das Wertpapierhandelsbilanzrecht mit daraus resultierender Kapitalmarktinformationsverantwortung hat insgesamt versagt. Hinzu kommt, dass die ESMA in einer *peer review* das zweistufige System sogar für gut befunden hat²⁹, so dass eine evtl. zu konstatierende Fehleinschätzung hinsichtlich der Markttauglichkeit des durch das BilKoG etablierten Systems auch auf internationaler Ebene zu verorten wäre.³⁰ Was den aufsichtsrechtlichen Aspekt und Vorwürfe gegenüber der BaFin betrifft, sie hätte früher und massiver auf die DPR einwirken müssen³¹: Es sei für den seitens der Legislative etablierten und nicht von der Exekutive zu verantwortenden Rechtsrahmen daran erinnert, dass etwa im Falle der Anerkennung einer Prüfstelle stichprobenartige Prüfungen gem. § 107 I 1 WpHG nur auf Veranlassung der Prüfstelle stattfinden; vgl. § 108 I 1 WpHG. Damit liegt aber auch nur eine Stichprobenkontrolle praktisch derzeit allein in den Händen der DPR.³² Schon dies ist hochproblematisch, weil in einer Konstellation, in der die geprüfte Rechnungslegung des Unternehmens nach An-

sicht der DPR keine Beanstandungen ergibt, der BaFin nur das Ergebnis der Prüfung mitzuteilen ist; vgl. § 342 b VI Nr. 3 HGB.

[14] Nach den Vorgaben des § 108 I 2 Nr. 2 WpHG kann die BaFin zudem ein solches Verfahren nur dann aufgreifen, wenn sie „erhebliche Zweifel“ an der Richtigkeit des Prüfungsergebnisses der Prüfstelle oder an der ordnungsgemäßen Durchführung der Prüfung durch die Prüfstelle hat. Damit folgt bereits auf der Wortlautebene, dass der Gesetzgeber gesteigerte Anforderungen an die Kontrolle der Prüfstelle durch die BaFin stellt, reichen einfache Zweifel doch gerade nicht aus.³³ Schon hinsichtlich der Glaubwürdigkeit der DPR wäre es lebensfremd anzunehmen, dass die BaFin im Hinblick auf erhebliche Zweifel an der Richtigkeit des Prüfungsergebnisses der DPR anders als *in praxi* zurückhaltend vorgehen wird. Es rächt sich an dieser Stelle, dass das Gesetz die DPR eben als unabhängige (*sic!*) erste Stufe des Enforcementverfahrens konzipiert hat. Auch wäre die Akzeptanz der Prüfstelle bei den – nicht kriminell agierenden – Unternehmen gefährdet und damit das gesamte Konzept des zweistufigen Enforcementverfahrens, wenn die BaFin die Arbeit der Prüfstelle als mit erheblichen Zweifeln behaftet ansehen würde, ganz ab-

²⁶ Die Wirecard AG als Einzelunternehmen sowie der Konzern legten für die Geschäftsjahre 2009 bis einschließlich 2018 jeweils einen testierten und mit einem uneingeschränkten Bestätigungsvermerk der hierfür mandatierten Wirtschaftsprüfungsgesellschaft versehenen Abschluss und Lagebericht vor. Keine der Abschlussprüfungen hat zu Einwendungen des Abschlussprüfers geführt. Regelmäßig wurde wirtschaftsprüferseitig festgestellt, dass nach Wirtschaftsprüfer-Beurteilung aufgrund der bei der Prüfung gewonnenen Erkenntnisse der Konzernabschluss den IFRS entspreche, wie sie in der EU anzuwenden sind, und den ergänzend nach § 315 a I HGB anzuwendenden handelsrechtlichen Vorschriften. Die WP-Gesellschaft stellte ferner für die Geschäftsjahre 2009 bis 2018 jeweils fest, der Konzernabschluss vermittele unter Beachtung dieser Vorschriften ein den tatsächlichen Verhältnissen entsprechendes Bild der Vermögens-, Finanz- und Ertragslage des Konzerns und auch der Konzernlagebericht stelle die Chancen und Risiken der zukünftigen Entwicklung zutreffend dar. Die übrigen in Presseberichten thematisierten Vorwürfe zu Bilanzmanipulationen wurden in den erteilten uneingeschränkten Bestätigungsvermerken weder erwähnt noch thematisiert; vgl. Sachstandsbericht des BMF (Fn. 11).

²⁷ Vgl. Sachstandsbericht des BMF (Fn. 11).

²⁸ Hierzu ausführlich *Wöbel/Mock*, Die Handels- und Steuerbilanz, 7. Aufl. 2020, S. 58 ff.

²⁹ ESMA, Peer review on guidelines in enforcement of financial information, 18.7.2017, abrufbar unter: <https://beck-link.de/hpn2m>.

³⁰ Daher ist der Peer Review Report der ESMA zum Fall Wirecard durchaus mit Vorsicht zu lesen – die ESMA spricht sich dort nicht – *quelle surprise* – gegen das zweistufige Verfahren mit seinen – auf der Hand liegenden – Schwächen aus und kann dies auch gar nicht, ohne sich zu sich selbst in Widerspruch zu setzen. Umso kritischer dürften die Aussagen der ESMA zu würdigen sein, die sie im Hinblick auf die anderen involvierten Institutionen (insb. DPR, BaFin, aber auch das BMF) trifft.

³¹ Vgl. dazu exemplarisch das Interview mit Frau MdBin Katja Hessel mit dem Deutschlandfunk vom 29.7.2020, abrufbar unter: <https://beck-link.de/km3hz>.

³² Schwark/Zimmer/Henrichs, Kapitalmarktrechts-Kommentar, 5. Aufl. 2020, § 108 WpHG Rn. 2.

³³ Wie hier Wissenschaftliche Dienste Deutscher Bundestag, Möglichkeiten der Bundesanstalt für Finanzdienstleistungsaufsicht zur Bilanzkontrolle von Unternehmen vor Abschluss der Prüfung durch die Deutsche Prüfstelle für Rechnungslegung DPR e. V. (WD 4 – 3000 – 070/20), 2.7.2020, S. 5, abrufbar unter: <https://beck-link.de/ckf4b>.

gesehen von – im Arbeitsalltag üblichen – Unstimmigkeiten.³⁴

[15] Die Frage, die sich stellt: Bilanzmanipulation ist wie erwähnt doch zugleich eine Marktmanipulation und zwar in einer der denkbar schwersten Begehungsformen. Warum hat die BaFin nicht nur das Enforcementverfahren nicht an sich gezogen, warum ging sie – diese Frage werfen Böcking/Gros in ihrem instruktiven Gutachten nicht auf – nicht separat wegen Marktmanipulation vor? Nach den §§ 106 ff. WpHG war ihr das jedenfalls nicht möglich. Dies deshalb, weil im WpHG das Enforcementverfahren als „Bilanzkontrolle“ eben als *lex specialis* gegenüber § 6 II, III 3 sowie §§ 11, 12 WpHG, welche die „Marktüberwachung“ ganz allgemein regeln, anzusehen sind, womit der BaFin aber im Rahmen des Enforcementverfahrens ausschließlich die in den §§ 106 ff. WpHG geregelten Befugnisse zukommen.³⁵ Dies gilt jedenfalls für Emittenten im regulierten Markt – bei Freiverkehrswerten greifen die §§ 106 ff. WpHG nicht.³⁶

[16] Aber der Reihe nach: Zunächst seien die sehr verdienstvollen Vorarbeiten des wissenschaftlichen Dienstes des Bundestages betreffend die Prüfungsmöglichkeit der BaFin gem. § 108 I 2 Nr. 2 WpHG vor Abschluss einer Prüfung von Finanzinformationen durch die Prüfstelle hervorgehoben: Es mag sich in der Tat die Frage stellen, ob, selbst beim Vorliegen „*erheblicher Zweifel*“ der BaFin gegenüber der Prüfstelle, diese schon während der Prüfung auf erster Stufe ein eigenständiges Prüfungsrecht der BaFin gem. § 108 I 2 Nr. 2 WpHG begründen können, oder erst der Abschluss der Bilanzkontrolle durch die Prüfstelle abgewartet werden muss. Insofern ist zu konstatieren: § 108 I 2 Nr. 2 Alt. 1 WpHG setzt nun einmal – unmissverständlich auf Wortlautebene – ein Prüfergebn voraus. Die Prüfung auf erster Stufe muss also abgeschlossen sein, damit es denklogisch überhaupt erst ein Ergebnis als dem letzten Schritt einer Prüfung geben kann. Damit scheidet eine vorherige Anwendbarkeit dieser Alternative aus. Demgegenüber verlangt § 108 I 2 Nr. 2 Alt. 2 WpHG erhebliche Zweifel an der ordnungsgemäßen Durchführung der Prüfung durch die DPR. Der Wortlaut lässt einen noch nicht abgeschlossenen Prüfungsprozess zu; systematisch zeigt der Vergleich zur ersten Alternative, dass § 108 I 2 Nr. 2 Alt. 2 WpHG keine Beschränkung auf ein abgeschlossenes Prüfverfahren durch die Prüfstelle erfahren sollte. Denn ein Prüfergebn wird dann fehlerhaft, wenn die Durchführung der Prüfung selbst fehlerhaft ist und ist gleichsam die unvermeid- wie unabweisbare Konsequenz einer fehlerhaften Durchführung. Eine Beschränkung des § 108 I 2 Nr. 2 Alt. 2 WpHG auf bereits abgeschlossene Prüfverfahren würde dazu führen, dass für diese Alternative kein eigener Anwendungsbereich gegenüber § 108 I 2 Nr. 2 Alt. 1 WpHG mehr existent wäre, weil ein fehlerhaftes Ergebnis eben eine

fehlerhafte Durchführung voraussetzt und der Gesetzgeber – insoweit konsequent – eine zweite Alternative gerade für laufende Prüfverfahren geschaffen hat. Daher spricht vieles dafür, dass schon vor Abschluss der Prüfung durch die Prüfstelle eine eigenständige Prüfung durch die BaFin nach § 108 I 2 Nr. 2 Alt. 2 WpHG jedenfalls grundsätzlich möglich sein soll.³⁷ Indessen muss die BaFin nach diesem Konzept „*erhebliche Zweifel*“ an einer ordnungsgemäßen Durchführung des Prüfverfahrens durch die DPR selbst haben, um insoweit rechtmäßig agieren zu können. Und woraus hätten sich in der *causa* Wirecard derartige Zweifel – an der Arbeit der DPR (*sic!*) – ergeben sollen? Um es zugespitzt zu formulieren: Die Arbeit des PUA mag entsprechende Erkenntnisse zu Tage fördern, aber über eine mangelhafte Tätigkeit der DPR hat die Financial Times jedenfalls nicht berichtet.

[17] Soweit nun namentlich der AKBR – und er tut dies fälschlicherweise – zu dem Schluss kommt, dass bei im Raum stehenden Betrugshandlungen eine ordnungsgemäße Durchführung der Prüfung durch die DPR nicht zu erwarten wäre und mithin die BaFin die Prüfung gem. § 108 I 2 Nr. 2 Alt. 2 WpHG an sich ziehen könne,³⁸ wäre zugleich das Fehlen einer gesetzlichen Regelung zu beklagen, wann (1) von einer fehlenden, die ordnungsgemäße Durchführung der Prüfung verhindernde freiwilligen Mitwirkung ausgegangen werden kann und (2) wann ein hinreichend konkretisierter Verdacht auf Bilanzmanipulationen besteht. Es wäre dann aber zugleich offen, wer insoweit eine finale Einschätzung treffen muss, losgelöst von der Frage der Einbeziehung der Prüfstelle in derartigen Fällen. Bei einer Entscheidungsbefugnis allein im Verantwortungsbereich der BaFin wäre es dieser überlassen, in konkreten Einzelfällen entweder ein zweistufiges Verfahren oder ein einstufiges Verfahren einzuleiten. Dies stünde jedoch im Widerspruch zum explizit erklärten Willen des Gesetzgebers, wonach das Enforcementverfahren als ein solches ausgestaltet ist, in dem die Emittenten zur Kooperation aufgerufen sind.³⁹ Auch bliebe außen vor, dass auch der jeweils in Rede stehende Emittent ein zentrales Interesse nicht nur haben kann, sondern haben wird (wenn er denn nicht grundsätzlich kriminell agiert),

³⁴ In diese Richtung auch Schwark/Zimmer/Henrichs, Kapitalmarktrechts-Kommentar, § 108 WpHG Rn. 7. Vgl. zur Prüfungsmöglichkeit der BaFin gem. § 108 I 2 Nr. 2 WpHG vor Abschluss der Prüfung durch die Prüfstelle unten Punkt IV.1.

³⁵ Vgl. Böcking/Gros, Gutachten zur Prüfung der Rechtsauffassung der BaFin, dass die DPR nach § 342b IV HGB auch dann auf erster Stufe prüfen muss und kann, wenn mögliche Betrugshandlungen (einschließlich möglicher Betrugshandlungen durch das Management) im Raum stehen, 11.10.2020, S. 51, abrufbar unter: <https://beck-link.de/n8bvd>.

³⁶ Hierzu unten Punkt IV.1.

³⁷ Vgl. Wissenschaftliche Dienste Deutscher Bundestag (Fn. 33), S. 5.

³⁸ So *Arbeitskreis Bilanzrecht Hochschullehrer Rechtswissenschaft* NZG 2020, 938 (944).

³⁹ Vgl. Entwurf eines Gesetzes zur Kontrolle von Unternehmensabschlüssen (Bilanzkontrollgesetz – BilKoG), BT-Drucks. 15/3421, S. 1, 11.

Vorwürfe im Hinblick auf eine Bilanzmanipulation oder einen Bilanzbetrug schnellstmöglich auszuräumen. Dann wird er aber eine Mitwirkung bei der Prüfung der Prüfstelle nicht verweigern, sondern er wird ganz im Gegenteil aktiv kooperieren.⁴⁰ Der kriminelle Emittent, um den es sich bei der Wirecard AG augenscheinlich gehandelt hat, stand dem – allzu gutgläubigen? – Gesetzgeber des BilKoG nicht vor Augen. Für diesen ist ein zweistufiges Verfahren, das auf Kooperation angelegt ist, fehlerhaft. Es sei sich schließlich vor Augen geführt, dass abseits von journalistischer Pressearbeit in den Referaten der Aufsicht ganz regelmäßig, um nicht zu schreiben: ständig Hinweise aus der Bevölkerung eingehen, die einen möglichen Bilanzbetrug eines Emittenten zum Gegenstand haben, gleich ob diese im regulierten Markt gelistet oder zum Handel in den Freiverkehr einbezogen sind.

[18] Das führt aber angesichts der doch recht eingeschränkten Möglichkeiten der §§ 106 ff. WpHG zu der Frage, welche Handlungsmöglichkeiten nach der allgemeinen Missstandsklausel des § 6 WpHG bei Emittenten, die im regulierten Markt gelistet sind, zur Verfügung stehen? Dies mag man sich bei erster unbedarfter Annäherung an die Rechtslage fragen und argumentieren, das AnSVG⁴¹ habe in Umsetzung der MarktmissbrauchsRL ein Vorgehen der BaFin wegen Marktmanipulation (in Form der Bilanzmanipulation) doch in jedem Fall ermöglichen wollen, eine Beschneidung oder gar eine Sperrwirkung der Befugnisse der BaFin durch das BilKoG habe hingegen nicht erzeugt werden sollen.

[19] Hier ist eine Lektüre der Gesetzgebungsmaterialien mehr als erhellend. Das BilKoG ist zunächst eine Reaktion auf den *Enron*-Skandal.⁴² Infolgedessen hat der deutsche Gesetzgeber für Deutschland durch das zweistufige System die in Europa vorhandenen Systeme miteinander kombiniert.⁴³ Er tat dies im Bewusstsein der europäischen Vorgaben, heißt es doch in der Begründung: *„Auch wenn die europäischen Systeme zur Durchsetzung der Rechnungslegung unterschiedlich sind, ist ihnen allen das Ziel gemein, die Integrität der Finanzmärkte und den Anlegerschutz zu stärken. Dieses Ziel verfolgt auch der Ausschuss der EU-Wertpapierregulierungsbehörden CESR (Committee of European Securities Regulators), der im März 2003 Grundsätze für die Ausgestaltung europäischer Enforcement-Systeme vorgelegt hat. Diese Grundsätze sind darauf angelegt, auf eine einheitliche Entwicklung der Enforcement-Systeme in Europa hinzuwirken.“*⁴⁴ Für den Fall, dass die BaFin möglicher krimineller Machenschaften gewahr wird, stellt sich der Gesetzgeber vor: *„Die Bundesanstalt ihrerseits hat Tatsachen, die den Verdacht einer Straftat im Zusammenhang mit der Rechnungslegung begründen, bei der für die Verfolgung zuständigen Behörde anzuzeigen. Zudem hat sie Tatsachen, die auf das Vorliegen einer Berufspflichtverletzung deuten,*

*an die Wirtschaftsprüferkammer und solche Tatsachen, die auf die Verletzung börsenrechtlicher Vorschriften schließen lassen, an die zuständige Börsenaufsichtsbehörde zu übermitteln. Eine gleich gelagerte Anzeigepflicht gegenüber den für die Verfolgung von Straftaten zuständigen Behörden und gegenüber der Wirtschaftsprüferkammer besteht für die private Prüfstelle.“*⁴⁵

[20] Keine Hinweise sind diesen Erläuterungen daraufhin zu entnehmen, die BaFin solle in strafrechtlich relevanten Fällen von den ihr in Konstellationen von vermutetem Marktmissbrauch zustehenden Befugnissen Gebrauch machen, die in der Sache einer Gefahrenabwehr dienen würden. Hinzu kommt der zeitliche Verlauf der beiden Gesetzgebungsverfahren von AnSVG und BilKoG, der quasi parallel erfolgte: so wurde der Regierungsentwurf des AnSVG⁴⁶ nur rund einen Monat vor dem des BilKoG⁴⁷ veröffentlicht und die beiden Gesetze wurden mit nur zweimonatigem Abstand im Bundesgesetzblatt veröffentlicht.⁴⁸ Trotz dieses Parallelismus ist aber nicht erkennbar, dass der Gesetzgeber auch nur daran dachte, der BaFin über einen Rückgriff auf die Generalklausel des damaligen § 4 WpHG (jetzt § 6 WpHG) – der durch das AnSVG erst neu geschaffen wurde und die an verschiedenen Stellen des WpHG enthaltenen Befugnisse der BaFin im Wege einer Generalklausel zusammenfasste⁴⁹ – im Enforcementverfahren, bei dem Hinweise auf strafrechtlich relevantes Verhalten zutage treten, mehr Befugnisse einzuräumen, als er dies in § 107 WpHG getan hat. Ganz im Gegenteil: § 107 V 1, 2 sowie VI 1, 3 WpHG, die § 6 VI 1 und XI 1, 3 entsprechen und teilweise (vgl. § 107 V 3, VI 2 WpHG) auf die Bestimmungen des § 6 WpHG verweisen, verdeutlichen vielmehr, dass der Gesetzgeber der BaFin für das Enforcementverfahren andere – weniger weitgehende – Befugnisse eingeräumt hat, als er dies der Behörde im Rahmen der allgemeinen Marktmissbrauchsaufsicht zugestanden hat. Dies tut er im Übrigen auch nicht durch den am 26.10.2020 vorgelegten Refe-

⁴⁰ Wie hier Böcking/Gros (Fn. 35), S. 11., denen der Verf. explizit folgt.

⁴¹ BGBl Abs. 1, Nr. 56 v. 29.10.2004, S. 2630.

⁴² Vgl. Entwurf eines Gesetzes zur Kontrolle von Unternehmensabschlüssen (Bilanzkontrollgesetz – BilKoG), BT-Drucks. 15/3421, S. 11: *„Nicht nur Unternehmensskandale in Übersee oder im europäischen Ausland – verursacht durch Bilanzfälschungen – haben gezeigt, welche massiven Auswirkungen solche Krisen haben können. Auch Krisen einzelner deutscher Unternehmen, die durch Manipulation der Abschlüsse verschleiert wurden, haben die Funktionstüchtigkeit des hiesigen Kapitalmarktes stark beeinträchtigt.“*

⁴³ Vgl. Entwurf eines Gesetzes zur Kontrolle von Unternehmensabschlüssen (Bilanzkontrollgesetz – BilKoG), BT-Drucks. 15/3421, S. 11.

⁴⁴ Vgl. ebd.

⁴⁵ Vgl. Entwurf eines Gesetzes zur Kontrolle von Unternehmensabschlüssen (Bilanzkontrollgesetz – BilKoG), BT-Drucks. 15/3421, S. 12.

⁴⁶ Entwurf eines Gesetzes zur Verbesserung des Anlegerschutzes (Anlegerschutzverbesserungsgesetz – AnSVG), BT-Drucks. 15/3174.

⁴⁷ Entwurf eines Gesetzes zur Kontrolle von Unternehmensabschlüssen (Bilanzkontrollgesetz – BilKoG), BT-Drucks. 15/3421.

⁴⁸ AnSVG im BGBl Abs. 1 Nr. 56 vom 29.10.2004, S. 2630, BilKoG im BGBl Abs. 1 Nr. 69 vom 20.12.2004, S. 2630.

⁴⁹ Entwurf eines Gesetzes zur Verbesserung des Anlegerschutzes (Anlegerschutzverbesserungsgesetz – AnSVG), BT-Drucks. 15/3174, S. 27

rentenentwurf des FISG⁵⁰, in dem § 107 WpHG ein neuer Absatz 7 angefügt wird, der die Regelung des § 6 XII WpHG übernimmt.

[21] Festhalten lässt sich damit, dass sich der Gesetzgeber bei der Ausgestaltung des Enforcementverfahrens am Leitbild eines kooperierenden Emittenten orientiert hat (er tut dies auch weiterhin im FISG) – das bei einer kriminellen Bande versagen muss – und dass er das Enforcementverfahren als spezielles Verfahren mit speziellen Befugnissen für die Behörde ausgestaltet hat (und dies auch weiterhin tut), ohne eine wie auch immer geartete Verbindung zu dem System der Verfolgung von marktmissbräuchlichem Verhalten herzustellen. Dies hätte jedoch aufgrund der Parallelität der Verfahren, dem Auslöser für die Schaffung des Enforcementverfahrens (der *Enron*-Skandal ist im Regierungsentwurf des BilKoG ja ausdrücklich genannt) und der Tathandlungen (Marktmanipulation *durch* Bilanzmanipulation) durchaus nahegelegen. Dass es trotz dieser naheliegenden Umstände zu diesen solchermaßen getrennten Systemen gekommen ist, lässt die Annahme zu, dass die Systeme getrennt bleiben sollten (und sollen), weil sie unterschiedliche Zielrichtungen haben. Wie der Gesetzgeber in der Begründung zum Regierungsentwurf des BilKoG ausdrücklich festhält, geht es ihm beim Enforcementverfahren in erster Linie darum, den Kapitalmarkt über Bilanzfehler zu informieren, indem diese veröffentlicht werden,⁵¹ dazu kann das Unternehmen erforderlichenfalls sogar verpflichtet werden. Allein über diese Mechanismen erhofft man sich die Wiederherstellung des Vertrauens des Marktes in die Richtigkeit von Unternehmensabschlüssen.⁵² Das Enforcementverfahren dient also nicht dazu, Marktmanipulation (in Form der Bilanzmanipulation) zu ahnden, sondern zur Überwachung der Einhaltung von Rechnungslegungsvorschriften. Strafrechtlich relevantes Verhalten (wegen Verstoßes gegen Rechnungslegungsvorschriften, vgl. zB § 331 HGB), das im Rahmen des Enforcementverfahrens zutage tritt, ist durch die dafür zuständigen Stellen zu ahnden, wie sich aus § 110 I WpHG und § 342 b XIII HGB ergibt, die jeweils eine Anzeigepflicht der BaFin bzw. der DPR vorsehen, wenn der Verdacht einer Straftat im Zusammenhang mit der Rechnungslegung eines Unternehmens besteht.

[22] Damit an Schwächen aber nicht genug: Auch auf der repressiven Seite weist das Enforcement-System weitere eklatante – gesetzgeberseitig zu vertretende – Konzeptionsfehler auf: So ist die BaFin etwa nur bei den Halbjahresfinanzberichten die zuständige Verfolgungsbehörde nach § 36 OWiG, nicht aber bei den Jahresfinanzberichten, die hier ja gerade in Rede standen.

[23] Rechtspolitisch erscheint es als eine *lesson learned* aus dem Fall Wirecard vertretbar, von dem zweistufigen Enforcementverfahren Abstand zu nehmen und ein einstufiges Verfahren zu etablieren, dessen Hoheit bei der

BaFin angesiedelt ist. Die Reibungsverluste zwischen den Instanzen sind naturgemäß – und nach den nicht von der Hand zu weisenden wie ehrlicherweise gemachten Lebenserfahrungen – schon sehr groß und haben augenscheinlich auch hier ein Handeln zu verhindern vermocht, das den Zielen des BilKoG gerecht geworden wäre. Das FISG springt hier zu kurz. Zwar wird das zweistufige System reformiert und der BaFin werden im Hinblick auf das Enforcementverfahren weitergehende Befugnisse eingeräumt wie etwa ein Durchsuchungsrecht der BaFin-Bediensteten in § 107 VII WpHG-E, wenn dies zur Wahrnehmung der Aufgaben nach § 106 WpHG-E erforderlich ist und konkrete Anhaltspunkte für einen erheblichen Verstoß gegen Rechnungslegungsvorschriften vorliegen.⁵³ Ein Eingreifen aufgrund einer „Gefahr im Verzug“ bei einer möglichen Marktmanipulation durch Bilanzmanipulation ist aber auch nach dem FISG in seiner Fassung bei Redaktionsschluss dieses Beitrages durch die BaFin-Bediensteten nicht praktikabel möglich.

[24] Dass eine Aufstockung des Personals bei der BaFin damit verbunden ist, versteht sich von selbst, sollte aber kein *show stopper* sein – die Aufsicht hat namentlich am Dienstsitz Frankfurt am Main in der Vergangenheit mehrfach bewiesen, dass sie solchen Großaufgaben gerecht wird, wenn man ihr nur die Möglichkeiten einräumt – erinnert sei etwa an die Übernahme der Zuständigkeit für die Billigung von Börsenzulassungsprospekten und die damit einhergehende Etablierung der Gruppe PRO (heute: Abteilung WA 5). Zudem sind der BaFin für eine effiziente Ahndung zur Erzielung general- wie spezialpräventiver Effekte die unabdingbaren Verfolgungskompetenzen legislativ einzuräumen – die Anstalt muss – selbstredend – auch die zuständige Verfolgungsbehörde nach § 36 OWiG für die Jahresfinanzberichte werden.

III. Marktmanipulation und Leerverkaufsverbote

1. Die Verfolgung von Marktmissbrauch durch die BaFin

[25] Die Rolle der Marktaufsicht nicht nur im *Dreyling'schen* Schnellbootssinne besteht insgesamt darin,

⁵⁰ Referentenentwurf eines Gesetzes zur Stärkung der Finanzmarktintegrität (FISG), S. 7, abrufbar unter: <https://beck-link.de/d6ynw>.

⁵¹ Entwurf eines Gesetzes zur Kontrolle von Unternehmensabschlüssen (Bilanzkontrollgesetz – BilKoG), BT-Drucks. 15/3421, S. 11, rechte Spalte, zweiter Absatz: „Ziel ist es, Unregelmäßigkeiten bei der Erstellung von Unternehmensabschlüssen und -berichten präventiv entgegenzuwirken und, sofern Unregelmäßigkeiten dennoch auftreten, diese aufzudecken und den Kapitalmarkt darüber zu informieren.“ [Hervorhebung durch Verf.]

⁵² Entwurf eines Gesetzes zur Kontrolle von Unternehmensabschlüssen (Bilanzkontrollgesetz – BilKoG), BT-Drucks. 15/3421, S. 1 und 11, rechte Spalte sowie linke Spalte oben: „Anleger reagierten auf Unternehmensskandale mit Zurückhaltung am Kapitalmarkt und entzogen ihm damit Liquidität (...)“

⁵³ Vgl. Referentenentwurf eines Gesetzes zur Stärkung der Finanzmarktintegrität (FISG) (Fn. 50), S. 7.

das reibungslose Funktionieren der Kapitalmärkte und ihre Integrität zu gewährleisten, um Vertrauen und Akzeptanz bei Investoren auf lokaler und globaler Ebene zu schaffen. Der Wirecard-Skandal hat die BaFin nicht nur hinsichtlich der Rechnungslegungsprüfung, sondern auch im Übrigen einer ganzen Reihe weiterer Vorwürfe ausgesetzt, die ihre Rolle als vertrauenswürdige Autorität, welche die Integrität der Wertpapiermärkte in Deutschland zu schützen hat, versucht in Frage zu stellen. Nicht zuletzt in der Tagespresse und im Nachhinein wird der Anstalt vorgehalten, Frühwarnungen vor Fehlverhalten der Wirecard AG vernachlässigt zu haben, als solche Behauptungen bereits 2015 von Journalisten der *Financial Times* in einer Artikelserie „House of Wirecard“ erhoben wurden. Am 1. Februar 2019 kam es seitens der BaFin schließlich zur Eröffnung von Untersuchungen wegen Marktmanipulation und später auch zu einer Abgabe an die StA München im Zusammenhang mit Berichterstattung der *Financial Times* wegen möglicher Marktmanipulation von Marktteilnehmern und falscher bzw. irreführender Angaben in der Finanzberichterstattung der Wirecard AG. Hier wird der BaFin vorgehalten, die Journalisten hätten die Arbeit der Aufsicht gemacht und „zum Dank“⁵⁴ seien sie angezeigt worden. Mittlerweile wird seitens der politischen Opposition das Unterfangen betrieben, den Journalisten, nachdem die StA München das Verfahren wegen Marktmanipulation eingestellt hat, das Bundesverdienstkreuz zukommen zu lassen.⁵⁵

[26] Insoweit bleibt festzuhalten: Auch das Verwenden zutreffender Informationen durch einen Journalisten mag eine Marktmanipulation begründen können. Die Rechtslage ist klar, wird aber von der Tagespresse beharrlich ignoriert. So existiert zwar das sog. Journalistenprivileg in Art. 21 MAR.⁵⁶ Hiernach sind – in Ablösung der Vorgängerregelung des Art. 1 Nr. 2 lit. c) Satz 2 der MarktmissbrauchsRL 2003 – bei der Beurteilung der Offenlegung und Verbreitung von Informationen für den Zweck von Art. 12 I lit. c) MAR die Regeln der Pressefreiheit und der Freiheit der Meinungsäußerung in anderen Medien sowie die journalistischen Berufs- und Standesregeln zu berücksichtigen, wenn die in Rede stehenden Informationen oder Empfehlungen für journalistische Zwecke oder anderen Ausdrucksformen in den Medien offengelegt oder verbreitet werden. So wird den entsprechenden grundrechtlichen Garantien der EuGRCh Rechnung gezollt.⁵⁷ Das ändert aber alles nichts daran, dass dieses sog. Journalistenprivileg jedenfalls dann nicht eingreift, wenn (1) den betreffenden Personen oder mit diesen in enger Beziehung stehenden Personen aus der Offenlegung oder Verbreitung der Information ein unmittelbarer oder mittelbarer Vorteil erwächst⁵⁸ oder wenn (2) die Weitergabe oder Verbreitung in der Absicht erfolgt, den Markt in Bezug auf das Angebot von Finanzinstrumenten, die Nachfrage danach oder deren Kurs irrezuführen.⁵⁹

[27] Vor diesem Hintergrund ist es grundsätzlich in keiner Weise zu beanstanden, dass die BaFin eine Anzeige gegen die Journalisten der *Financial Times* erstattet hat – sie wird nach Aktenlage ihre guten Gründe gehabt haben und ein kapitalmarktrechtlicher Freibrief für bestimmte Parteien und Beteiligte in der *causa* Wirecard existiert nicht und wäre für das Vertrauen in die Integrität der Märkte insgesamt auch fatal. Dem steht auch nicht entgegen, dass die StA München das Ermittlungsverfahren wegen Vorwürfen der Marktmanipulation zwischenzeitlich eingestellt hat – im Zusammenspiel zwischen StA und BaFin sind divergierende Auffassungen hinsichtlich der Ahndungswürdigkeit eines kapitalmarktrechtlichen Verhaltens gang und gäbe wie auch erwartbar. Dies ist in einem Rechtsstaat von den Betroffenen auszuhalten. Es ist vielmehr begrüßenswert, dass die BaFin in alle Richtungen ermittelt und vielfältig Aktivitäten entfaltet hat. Dies ist gerade von ihr zu erwarten. Das Verfahren wegen Insiderhandel gegen die Journalisten läuft bei Schlussredaktion dieses Beitrags noch. Womöglich haben die hinter der Wirecard AG stehenden Akteure die Journalisten auch über entsprechende Quellen mit „Informationen gefüttert“, um sie „in einen Insiderhandel zu treiben“, wie verschiedentlich kolportiert wird. Dies kann vom Schreibtisch des Verfassers nicht abschließend aufgeklärt werden, wäre dies so, wäre es aber vor allem eines: für die Journalisten mutmaßlich strafbar. Es bleibt zu hoffen, dass die mögliche Vergabe des Bundesverdienstkreuzes sich bis zur Klärung dieser Umstände noch hinziehen mag. Ausweislich des Sachstandsberichts des BMF dürfte die BaFin in Fragen der Marktmissbrauchsrechts angesichts der Vielzahl der dort verzeichneten Maßnahmen sachgerecht vorgegangen sein – oder um im *Dreyling'schen* Bild zu bleiben: dieses Schnellboot hat „performed“.

2. Leerverkaufsverbote

[28] Darüber hinaus erließ die BaFin vor dem Hintergrund zahlreicher Hinweise auf Marktmanipulation und Insiderhandel rund um die Wirecard AG am 18. Februar 2019 ein zweimonatiges Leerverkaufsverbot für Aktien der Wirecard AG, welches durch die ESMA nicht beanstandet wurde. Auch diese Maßnahme erfuhr vielfältige Kritik unter Hinweis darauf, dass Investoren die mit dem Leerverkaufsverbot einhergehenden Beschränkung immer noch als ein Zeichen der Unterstützung für Wirecard seitens der BaFin interpretiert haben

⁵⁴ Vgl. Twitter-Post des MdB Danyal Bayaz vom 5.11.2020, abrufbar unter: <https://beck-link.de/k5zt2>.

⁵⁵ Vgl. Twitter-Post des MdB Danyal Bayaz vom 3.9.2020, abrufbar unter: <https://beck-link.de/x7428>.

⁵⁶ Vgl. hierzu etwa Schwark/Zimmer/Kumpant/Schmidt, Kapitalmarktrechts-Kommentar, Art. 21 MAR Rn. 5 ff.

⁵⁷ Vgl. Erwägungsgrund 77 MAR.

⁵⁸ So auch schon früher Art. 1 Nr. 2 lit. c) Satz 2 der MarktmissbrauchsRL 2003 aE.

⁵⁹ Klöhn/Schmolke, MAR, 2018, Art. 12 Rn. 272.

(könnten), auch hätten Fondsmanager Verluste hinnehmen müssen. Zu Recht?

[29] Leerverkäufe bestimmten in jüngster Zeit die Schlagzeilen immer dann, wenn börsennotierte Gesellschaften Opfer von sog. *Short Seller*-Attacken wurden mit drastischen negativen Auswirkungen auf den Börsenkurs, wie dies bekanntlich neben *Wirecard* etwa auch *Ströer*, *Aurelius* und Anfang März 2018 auch bei *ProSiebenSat 1* und in jüngster Zeit bei *Grenke* der Fall war.⁶⁰ Die Attraktivität zur Vornahme von Leerverkäufen für Kapitalmarktakteure ist immens, wobei der Umstand, dass Leerverkäufe nicht per se etwas schlechtes und verbotswürdiges Verhalten sind, die Beurteilung und angemessene Rechtsbehandlung nicht vereinfachen. Was macht das Geschäftsmodell von *Short Seller*-Attacken aus und welche Verteidigungsmöglichkeiten bestehen ganz grundsätzlich für betroffene Emittenten? Zunächst ist dieses *business concept* bereits dadurch nahezu simpel, als es lediglich drei Schritte erfordert:

1. einen Leerverkauf von Aktien der Zielgesellschaft;
2. die Veröffentlichung negativer Nachrichten über eben diese Gesellschaft und
3. die Eindeckung mit den im Kurs gesunkenen Aktien der Gesellschaft zur Erfüllung der Verpflichtung aus dem Leerverkauf respektive aus dem Deckungsgeschäft.⁶¹

[30] *Short Seller* haben vor dem Hintergrund dieser Orchestrierung von Marktakteuren einen nahezu diametral entgegengesetzten Anlass – ihnen geht es darum, einen möglichst niedrigen Kurs (*Shareholder Value Minimization*) ohne eine Aktionärsstellung mit Mitgliedschaftsrechten fruchtbar zu machen. Gängig wie zutreffend ist daher auch die mitunter zu lesende Bezeichnung *Activist Investors*.⁶²

[31] Das frappierende an der phänomenologischen Situation: Sie ist nicht *per se* illegal. Vielmehr lassen sich der Leerverkaufs-VO gerade Anforderungen entnehmen, die eine erlaubte und sogar regulatorisch gewünschte Tätigkeit von *Short-Selling* zulassen.⁶³ Zu erinnern ist an die *Short Selling*-Attacke auf *Wirecard* aus dem Jahr 2016: Auf der von der *Zatarra Research & Investigations LLC* verantworteten Website erschien ein über 100 Seiten starker Bericht, in dem heftige Vorwürfe gegen Führungskräfte von *Wirecard* (Geldwäsche, Umgehung des US-Verbots von Online-Glücksspiel etc.). Effekt des *Zatarra*-Berichts war ein Kurssturz von EUR 42 auf EUR 33. Indessen unterhielt keiner der Hedgefonds, die nach den Transparenzvorschriften Nettoleerverkaufspositionen veröffentlicht hatten, eine (offenkundige bzw. bekannt gewordene) Verbindung zu *Zatarra*.⁶⁴ Auch soll die *Wirecard AG* selbst im Jahr 2019 Opfer eines Erpressungsversuchs geworden sein. So bestätigte die StA München gegenüber dem Handelsblatt, am 15. Februar 2019 „*erstzunehmende Informa-*

tionen von Wirecard erhalten [zu haben], dass eine neue Shortattacke geplant ist und dass mit viel Geld versucht wird, Medienberichterstattung zu beeinflussen“. Die Kursreaktionen fielen entsprechend heftig aus.⁶⁵

[32] Die Situation für die Aufsichtsbehörde ist knifflig und Gegenstand einer derzeit lebhaft geführten kapitalmarktrechtlichen Debatte, in der einschlägige Instrumente diskutiert werden.⁶⁶ In Betracht kommt für ein öffentlich-rechtlich getriebenes Krisenmanagement aber eben auch ein Instrumentarium, was *de lege lata* schon bereit steht:⁶⁷ So hat die BaFin gem. § 6 II 4 WpHG eben das Recht, den Handel mit einzelnen oder mehreren Finanzinstrumenten vorübergehend zu untersagen oder die Aussetzung des Handels in einzelnen oder mehreren Finanzinstrumenten an Märkten, an denen Finanzinstrumente gehandelt werden, anzuordnen, soweit dies zur Durchsetzung der Verbote und Gebote des WpHG oder der MAR bzw. zur Beseitigung von Missständen gem. § 6 I WpHG angezeigt ist⁶⁸. Darüber

⁶⁰ Die Anzeichen dafür, dass es sich hierbei nicht um vereinzelte Vorfälle, sondern um ein im Vordringen befindliches neues Geschäftsmodell handelt, liegen auf der Hand; vgl. *Wentz WM* 2019, 196 ff.

⁶¹ Für *Short Seller* besteht aufgrund derartiger Attacken die Möglichkeit zur Erzielung exorbitanter Profite, die betroffene Zielgesellschaft sieht sich mit der unangenehmen Situation konfrontiert, dass ein Leerverkaufsvolumen besteht und dass sie spätestens nach der Veröffentlichung von negativen Informationen auf mehreren kapitalmarktrechtlichen Baustellen betreffend die Kommunikation mit den Marktteilnehmern und auf der Investors Relations-Ebene gefordert ist. Phänomenologisch ist dabei nicht zu verkennen, dass es einen Gegenpol aktivistischer *Short Seller* zu sog. aktivistischen Aktionären gibt.

⁶² *Graßl/Nikoleyczik AG* 2017, 49 (51).

⁶³ So müssen – anknüpfend an die eingegangene Leerverkaufsposition – Halter einer Netto-Leerverkaufsposition in Aktien bzw. Verwaltungseinheiten oder bestimmte Unternehmen innerhalb einer Unternehmensgruppe nach Art. 6 der Leerverkaufs-VO ihre Nettoleerverkaufspositionen in Aktien gegenüber der Öffentlichkeit offenlegen, wenn diese Positionen den Schwellenwert von 0,5 % des ausgegebenen Aktienkapitals des betreffenden Unternehmens erreichen, über- oder unterschreiten; oberhalb dieses Schwellenwerts sind Veränderungen in Intervallen von 0,1 % des ausgegebenen Aktienkapitals des betreffenden Unternehmens offenzulegen; vgl. *Just/Voß/Ritz/Becker/von Buttlar/Petersen, WpHG*, § 30 h Rn. 20; *Mülbelt/Sajnovits ZBB* 2012, 266 (281). Nun darf aber der Research Report als zweites benötigte Element für eine wirtschaftlich lukrative *Short Seller*-Attacke dann negative Aussagen bzw. Einschätzungen zur Lage der Gesellschaft und ihrer Geschäftstätigkeiten enthalten. Insoweit kann in der Folge den Leerverkäufer gem. Art. 20 I MAR (VO (EU) Nr. 596/2014) in Anknüpfung an die veröffentlichte Analyse eine Verpflichtung treffen, Interessenkonflikte bezüglich der Finanzinstrumente, auf die sich die Informationen beziehen, offenzulegen. Die in Rede stehenden Finanzinstrumente wären namentlich insbesondere die *Short*-Positionen der Leerverkäufer. Bei den veröffentlichten Informationen muss es sich um Anlageempfehlungen oder Anlagestrategieempfehlungen handeln; vgl. Art. 3 I Nr. 34, 35 MAR.

⁶⁴ Hinzu kommt, dass der *Zatarra*-Bericht durch eine sehr professionelle und aufwendige Gestaltung auffällt. Vermutungen, dass er von Leerverkäufern finanziert wurde, erscheinen daher nicht gänzlich aus der Luft gegriffen.

⁶⁵ Zwischen dem 30.1.2019 und dem 15.2.2019 fiel der Kurs von 167,00 € (Startkurs 30.1.2019) auf 99,90 € (Schlusskurs am 15.2.2019), was für die Marktkapitalisierung eine Reduzierung um 40 % bedeutete. In den drei Monaten vor dem 29.1.2019 betrug die historische Volatilität des Börsenkurses der *Wirecard AG* 49,13 %.

⁶⁶ Vgl. nur *Möllers NZG* 2018, 649 ff.; *Klöhn/Mock/Voß, FS 25 Jahre WpHG*, S. 745 ff.; *Mülbelt/Sajnovits BKR* 2019, 313 ff.; ferner *Schockenhoff WM* 2020, 1349 ff.

⁶⁷ In diese Richtung denkt auch *Mülbelt ZHR* 182 (2018), 105 (112).

⁶⁸ Gemeint ist etwa die ordnungsgemäße Durchführung des Handels mit Finanzinstrumenten.

hinaus kann die BaFin bzw. die jeweilige Börsenaufsicht bei einem signifikanten Kursverfall innerhalb eines Handelstages gegenüber der Schlussnotierung des Vortags nach Art. 23 der LeerverkaufsVO sogar gedeckte Leerverkäufe von Finanzinstrumenten zumindest befristet beschränken (sog. *circuit breaker*). Wenn der Mut zur Inanspruchnahme dieser Instrumente in der Aufsichtspraxis besteht und eine rechtmäßige Handhabung überzeugend gelingt, mag hier sogar der Schlüssel für die Zukunft der effizienten Bekämpfung von *Short Seller*-Attacken liegen. Und genau dies ist hier in der Praxis passiert. Man mag mit der Begründung der entsprechenden Verfügung der BaFin hadern⁶⁹ und sich eine ausführlichere Prüfung der Verhältnismäßigkeit im engeren Sinne wünschen⁷⁰ – am Ende des Tages hat die Aufsicht nach hier vertretener Auffassung insoweit rechtskonform und zielgerichtet gehandelt. Auch durch die Handhabung dieser Instrumente lässt sich ein Vertrauen in das Funktionieren des Kapitalmarktes herstellen. Ein milderer Mittel stellt zwar in jedem Fall die Aussprache einer Warnung gem. § 6 II 3 WpHG dar, was bei derartigen Volatilitäten aber bereits kein (geeignetes) Mittel mehr sein mag.

IV. Die wertpapierhandelsrechtliche Crux des § 6 WpHG – was heißt dies für Freiverkehrswerte?

[33] So weit, so gut oder auch so schlecht, je nach Sichtweise – was bleibt nun für die Freiverkehrswerte? Das ist das Segment, in dem für zahlreiche FinTechs für die Kapitalaufnahme abseits erfolgreich abgeschlossener Seed-Runden die Musik für die Kapitalaufnahme beim Publikum spielt. Und es sei sich nichts vorgemacht: Das nächste Wirecard wird nach kriminalistischer Lebenserfahrung schon auf der Lauer liegen – das Geldwäschegewerbe dürfte für gewisse Kreise wirtschaftlich einfach zu attraktiv sein, als das neue Akteure nicht auf den Versuch der Etablierung einer neuen „Waschmaschine“ verzichten würden. Die Spur, ob die BaFin bei wertpapierhandelsrechtlich auffälligem Verhalten und insbesondere bei behauptetem Bilanzbetrug früher tätig werden kann, als dies bei der Wirecard AG als einem Unternehmen im regulierten Markt der Fall war, führt nach den obigen Ausführungen⁷¹ für Freiverkehrswerte allein zu §§ 6, 11, 12 WpHG und damit zur allgemeinen wertpapierhandelsrechtlichen Missstandsaufsicht.⁷²

1. Vorgaben des § 6 WpHG

[34] Wie aufgezeigt, enthält das WpHG in den §§ 106 ff. für die Bilanzkontrolle spezielle normative Vorgaben. Diese beziehen sich indessen ausschließlich auf Emittenten, für welche die Bundesrepublik Deutschland Herkunftsstaat ist, daher finden sie auf Emittenten, deren Wertpapiere ausschließlich in den Freiverkehrs-

handel einbezogen sind, keine Anwendung. Kann die BaFin daher zur Überprüfung eines Jahresabschlusses und einer mit der Aufstellung eines eventuell unrichtigen Abschlusses verbundenen Marktmanipulation auf § 6 WpHG zurückgreifen und anordnen, dass die Abschlüsse von in den Handel im Freiverkehr einbezogenen Emittenten durch einen Wirtschaftsprüfer prüfen zu lassen? Dies wäre für FinTechs, zu denen entsprechende Hinweise eingehen, ein scharfes Schwert. Insoweit spielt auch das Konkurrenzverhältnis des § 6 WpHG zu den §§ 106 ff. WpHG keine Rolle.

[35] Zunächst räumt § 6 III 1 WpHG der BaFin Auskunftsrechte gegenüber jedermann ein; zudem ermöglicht es die Norm, neben Unterlagen auch die Vorlage von Daten und die Überlassung von Kopien zu verlangen sowie Personen zu laden und zu vernehmen, um die Einhaltung der Verbote und Gebote unter anderem des WpHG oder der MAR zu überwachen. Zudem ist in § 6 II 1, 2 WpHG eine Generalklausel enthalten, nach welcher die BaFin Anordnung treffen darf, die zur Durchsetzung der Einhaltung der Ge- und Verbote des WpHG sowie bestimmter in § 1 I Nr. 8 WpHG aufgezählte europäischer Verordnungen darunter unter anderem auch der MAR geeignet und erforderlich sind.⁷³

⁶⁹ Man mag auch in Frage stellen, ob die *Wirecard AG* tatsächlich als „wichtig für das globale Finanzsystem angesehen“ werden kann, wie es in der Allgemeinverfügung der BaFin explizit heißt. Zumindest hat die BaFin es mit dem Erlass des Verbotes versäumt darzulegen, aus welchen tatsächlichen Fakten sich eine solche derartige Wichtigkeit für das Finanzsystem ergeben soll und welche Ermittlungen sie dahingehend angestellt hat. Der Bedeutungsgrad von *Wirecard* wird in dem Bescheid schlechthin unterstellt. Anders verhält es sich hingegen in der ESMA-Opinion, die dezidiert Anhaltspunkte dafür zusammenträgt, warum im verfahrensgegenständlichen Fall eine derartige Relevanz gegeben sein kann, nämlich vor dem Hintergrund, dass die *Wirecard Bank AG* Inhaberin einer Banklizenz nach dem deutschen KWG ist sowie die *Wirecard Solutions Limited* eine E-Geld-Erlaubnis der FCA nach britischem Zahlungsdienstrecht hält. Vgl. Ziff. 32 der ESMA-Opinion: „The potential impact on the financial system are based on *Wirecard's* status as a payment service provider with a network of connections to customers in multiple economic sectors, among them the banking sector. Moreover, ESMA notes that *Wirecard* operates through subsidiaries in the US market (*Wirecard North America*), Brazil (*Wirecard Brasil*) and Asia (*Wirecard Asia Pte Ltd.*), and is the parent company of *Wirecard Card Solutions Limited*, a firm that received permission by the UK Financial Conduct Authority to issue electronic money (e-money) and provide payment services. ESMA notes as well that BaFin has expressed concerns about the possibility of similar practices (in case the suspicions of market manipulation were confirmed) extending to other DAX 30 issuers some of which are financial institutions and market infrastructure providers.“

⁷⁰ Krit. etwa auch Müllert/Sajnovits BKR 2019, 313 (317); Klöhn/Mock/Voß, FS 25 Jahre WpHG, S. 745 ff.

⁷¹ Vgl. Punkt II.2.

⁷² Die aufsichtsrechtlichen Generalklauseln haben in jüngster Zeit vielfach eine Ausdehnung erfahren und geben mitunter, wenn man sich mit ihnen näher befasst, ganz überraschende Befugnisse her. Den Maßstab setzt derzeit § 5 KAGB, eine Norm, die sogar Doppelungen enthält und von der Reichweite der behördlichen Befugnisse sogar das KWG auszusteichen vermag; vgl. Emde/Dornseifer/Dreibus/Emde, Kapitalanlagegesetzbuch, 2. Aufl. 2019, § 5 KAGB Rn. 8; ihm folgend Arndt/Voß/Bruchwitz/Voß, Recht der Alternativen Investmentfonds, 2021, § 5 KAGB Rn. 7 (im Erscheinen).

⁷³ Die Vorgaben des 6 II, III WpHG waren bis zur Neunummerierung durch das 2. FiMaNoG in § 4 WpHG aF enthalten, der durch das AnsVG mit Wirkung vom 30.10.2004 in das WpHG eingefügt wurde.

a) § 6 II, III WpHG als Grundlage für die Anordnung der Prüfung eines Jahresabschlusses eines Freiverkehrsemittenten?

[36] Indessen kommen § 6 II, III WpHG als Ermächtigungsgrundlage für eine Anordnung der Prüfung eines Jahresabschlusses eines Freiverkehrsemittenten nur dann in Betracht, wenn diese Prüfung der Aufklärung einer Marktmissbrauchshandlung nach der MAR dient. Somit wäre im Rahmen einer solchen Untersuchung gewissermaßen als Vorfrage auch die Überprüfung der Richtigkeit des Jahresabschlusses eines in den Handel im Freiverkehr einbezogenen Emittenten grundsätzlich möglich. Dazu müssten der BaFin im konkreten Fall ausreichende Anhaltspunkte für einen eventuell gegebenen Verstoß gegen das Marktmanipulationsverbot der Art. 12 und 15 MAR vorliegen.

[37] Worin solche ausreichenden Anhaltspunkte liegen könnten, sind § 6 II, III WpHG auf Wortlautebene jedenfalls nicht zu entnehmen. Es erscheint vertretbar, sich wegen der inhaltlichen Sachnähe an den Vorgaben des § 107 I 1 WpHG zu orientieren, geht es doch auch dort um die Möglichkeit einer Bilanzprüfung. Man wird verlangen müssen, dass konkrete Anhaltspunkte für einen Verstoß gegen Rechnungslegungsvorschriften gegeben sind und diese auch auf Umstände tatsächlicher Art zurückzuführen sind, so dass bloße Vermutungen, Spekulation oder Hypothesen nicht ausreichen, um ein behördliches Eingreifen zu rechtfertigen.

[38] Für ein Nutzbarmachen des § 6 WpHG geht es also um die Frage, ob falsche oder irreführende Signale iSd Marktmanipulationsverbots gegeben sind. Lässt sich die Möglichkeit einer Marktmanipulation aufgrund fehlerhafter Rechnungslegung vermuten, so wäre an die Anordnung gegenüber dem in Rede stehenden Emittenten zu denken, die Prüfung der einschlägigen Unternehmensabschlüsse bzw. ausgewählter Teile dieser Abschlüsse durch einen Wirtschaftsprüfer vornehmen zu lassen. Ist so etwas unter dem Regime des § 6 WpHG rechtmäßig möglich?

[39] Sowohl § 6 III 1 WpHG als auch § 6 II 2 WpHG sind als Ermessensnormen konzipiert, so dass eine behördliche Maßnahme zur Aufklärung ob ggf. eine – auch nur mögliche – Marktmanipulation durch eine Bilanzmanipulation sich an den Vorgaben des Verhältnismäßigkeitsgrundsatzes messen lassen muss. Zunächst mag es auf Basis von § 6 III 1 WpHG zu diesem Zweck möglich sein, von jedermann u. a. Auskünfte, Unterlagen sowie die Vorlage von Daten und die Überlassung von Kopien zu verlangen sowie Personen zu laden und zu vernehmen. Dies beinhaltet jedoch ersichtlich nicht die Anordnung der Tätigkeit eines Wirtschaftsprüfers, so dass diese Norm als taugliche Ermächtigungsgrundlage ausscheidet.

[40] Demgegenüber ermöglicht es § 6 II 2 WpHG, Anordnungen zu treffen, die zur Durchsetzung der Einhaltung der Ge- und Verbote des WpHG, der aufgrund des WpHG erlassenen Rechtsverordnungen sowie der in § 1 I Nr. 8 WpHG genannten europäischen Verordnungen, also insbesondere der MAR, geeignet und erforderlich sind. Trifft die BaFin eine Anordnung zur Prüfung von Jahresabschlüssen oder ausgewählter Teile, so dient die Feststellung eines allfälligen Bilanzfehlers der Klärung der Vorfrage, ob möglicherweise eine Marktmanipulation gegeben ist, was wiederum im Anschluss an die Feststellung des Bilanzfehlers in einer weiteren Untersuchung zu klären wäre. Unabhängig davon, ob eine auf § 6 II 2 WpHG gestützte Anordnung überhaupt geeignet, erforderlich und angemessen wäre, ist jedoch zunächst zu beleuchten, ob eine solche Anordnung praktisch durchgesetzt werden könnte, um die Ziele des Gesetzes zu erreichen.

b) Praktische Durchsetzbarkeit

[41] In Rechnung zu stellen ist zunächst, dass die BaFin grundsätzlich sehr zügig handeln müssen, damit ihre Maßnahmen noch als geeignet eingestuft werden können.

[42] Vor Erlass eines entsprechenden Verwaltungsaktes ist zunächst eine Anhörung nach Maßgabe des § 28 VwVfG durchzuführen, in der dem betroffenen Emittenten mitzuteilen ist, dass behördenseitig die Anordnung der Prüfung seiner Abschlüsse durch einen Wirtschaftsprüfer beabsichtigt sei. Allerdings ist zu bedenken, dass dann, wenn mit krimineller Energie verfasste vorsätzliche Fälschungen von Unternehmensabschlüssen in Rede stehen sollten, sich ein Emittent allein aus Gründen der Zeitgewinnung vor den Verwaltungsgerichten zur Wehr setzen wird. Auch Verfahren des einstweiligen Rechtsschutzes erreichen vor dem für die BaFin zuständigen VG Frankfurt am Main nicht selten eine Verfahrensdauer von mehr als sechs Monaten, bis der Verfahrensstand ausgeschrieben ist (*in praxi* häufig bis zur Quadruplik).

[43] Ignoriert das Unternehmen die – ggf. gerichtlich bestätigte – Prüfungsanordnung, müsste die BaFin Verwaltungszwang zum Einsatz bringen. Dieser muss separat angeordnet werden und seine Durchsetzung beansprucht einen Zeitraum, der namentlich bei Konstellationen, in denen eine behauptete Bilanzmanipulationen durch die Presse publik gemacht worden sind, für ein effizientes Verwaltungshandeln insgesamt nicht zur Verfügung steht.

[44] Zudem dürfte sich ein auf § 6 II 2 WpHG gestütztes Vorgehen gegenüber Freiverkehrsemittenten dem validen Vorwurf ausgesetzt sehen, aufgrund der mit solchen Prüfungen verbundenen Kostenträgungen

schlechthin unbillig zu sein. Und dies ist schlagend: Wird einem Unternehmen *qua* Anordnung „ein Wirtschaftsprüfer zugewiesen“, stellt sich die Frage, wer denn für die Kosten des Unterfangens aufkommt. Es sind mehrere Wege einer Anordnung denkbar: Dem Unternehmen wird aufgegeben, einen Wirtschaftsprüfer zu mandatieren oder, falls dies nicht verfängt, die BaFin mandatiert einen Prüfer im Wege der Ersatzvornahme. Indessen ist anders als in § 17c FinDAG für die in §§ 106 ff. WpHG geregelten Konstellationen keine gesonderte Kostenerstattung durch den betroffenen Emittenten vorgesehen. Konsequenterweise fielen die Kosten eines durch die BaFin bestellten Prüfers dann allen Freiverkehrsemitenten in ihrer Gesamtheit zur Last, und zwar über die nach §§ 16, 16 i I 1 Nr. 2 FinDAG zu entrichtende Umlage. Dies dürfte jedoch schlechthin unbillig sein, wird so doch das gebührenrechtlich maßgebliche Verursacherprinzip missachtet.⁷⁴

[45] Faktisch bleibt der BaFin daher derzeit nichts anderes übrig, als solche Fälle bei ausreichenden Anhaltspunkten – und auch nur dann – an die Staatsanwaltschaften weiterzugeben, damit sich diese, ggf. auch im Hinblick auf andere Straftatbestände, mit den ihnen eingeräumten Befugnissen (Durchsuchung etc.) der Sachverhalte annehmen – es sei denn, der Gesetzgeber entscheidet sich für eine Verlagerung von Zuständigkeiten oder eine Doppelung der Befugnisse bei der BaFin.

2. Zwischenergebnis

[46] Auch wenn die Anordnung von Prüfungen von Jahresabschlüssen von Freiverkehrsemitenten aufgrund der wertpapierhandelsrechtlichen Generalklausel geeignet, erforderlich und angemessen sein sollte, fehlte ihr es jedoch an der zu fordernden Praktikabilität. Die BaFin wird zum einen nicht hinreichend zügig agieren können, zum anderen würde eine entsprechende Anordnung zu einer unbilligen Kostentragungspflicht führen.

V. Fazit

[47] Unser Durchmarsch durch die Wirecard-Affäre hat gezeigt, dass die BaFin eine Vielzahl von Maßnahmen ergriffen hat. So leitete sie insbesondere vielfach Untersuchungen möglicher Marktmanipulationen und vermuteten Insiderhandels durch Marktteilnehmer ein, es gab eine Untersuchung möglicher Marktmanipulationen durch die Wirecard AG, es wurde ein Bußgeld in Höhe von EUR 1,52 Mio. gegen die Wirecard AG wegen zu später Vorlage von Finanzberichten verhängt, es gab regelmäßige Gespräche mit der DPR und ausweislich des Sachstandsberichts des BMF auch ein nur als konsequent zu bezeichnendes Handeln gegenüber der

Wirecard AG nach Aufdeckung der Bilanzprobleme durch die KPMG-Sonderprüfung. Weiter hat die BaFin dabei u. a. wegen des starken Auslandsbezugs die Kooperation mit mehreren ausländischen Behörden gesucht sowie Erkenntnisse und Informationen an die jeweils zuständige Staatsanwaltschaft bzw. Auslandsbehörde weitergegeben. Gleichwohl hat sich – unabweisbar – gezeigt, dass dies im Ergebnis nicht gefruchtet hat. Hat die BaFin deshalb versagt? Ganz im Gegenteil, sie hat an Recht und Gesetz gebunden nach hier vertretener Auffassung als Exekutive das gemacht, wozu sie berufen ist – sie hat die gegenwärtigen Kontrollstrukturen vollzogen. Dass diese insgesamt nicht ausreichend waren, um ein mutmaßliches System betrügerischer Strukturen frühzeitig aufzudecken, ist allenfalls der Legislative anzulasten, die den erklärten Zielen des BilKoG zum Trotz ein Enforcement-System etabliert hat, dessen strukturelle Schwächen auf der Hand liegen und überdies ein Vorgehen nach marktmanipulationsrechtlichen Befugnissen gewissermaßen sperrt, bis es zu einem Abschluss gekommen ist. Ermächtigungsgrundlagen für ein Vorgehen der BaFin bei „Gefahr im Verzug“ in der Konstellation einer möglichen Marktmanipulation durch Bilanzmanipulation existieren nicht. Versäumnisse oder gar ein „Versagen“ der Aufsicht, wie es in der tagespolitischen Hektik mitunter deklamiert wird, ist nach dem öffentlich bekannten Sachverhalt jedenfalls nicht festzustellen. Sie dürfte nicht zuletzt jedenfalls nach den Informationen, die öffentlich bekannt sind, sogar im Einklang mit dem von ihr eingangs – bewusst provokant – zitierten Wertekanon gehandelt haben.

[48] Klar ist auch, dass es einen hundertprozentigen Schutz gegen kriminelles Verhalten gerade auf den Finanzmärkten niemals geben wird. Gleichwohl muss Kriminalität mit allen rechtstaatlichen Mitteln präventiv wie repressiv begegnet werden und dazu gehört eben auch, ausreichend strikte Kontroll- und Aufsichtssysteme vorzusehen. Hinsichtlich des Wertpapierhandelsbilanzrechts scheinen – anders als für das Marktmanipulationsrecht – erweiterte Kompetenzen angezeigt, die im Freiverkehr namentlich auch aufstrebende FinTechs betreffen werden. Neben der Etablierung eines einstufigen Enforcementverfahrens sollte eine Generalklausel vorgesehen werden, die – anders als der gegenwärtige § 6 WpHG – der BaFin jedenfalls anlassbezogen ein zügiges Agieren ermöglicht. Das bisher zur Verfügung gestellte Instrumentarium dürfte bedauerlicherweise nicht hinreichend praktikabel sein. Auch das FISG schafft hier nicht die Verbesserungen, die geboten sind. Zwar hat der Gesetzgeber infolge der Wirecard-Vorkommnisse zutreffend erkannt, „dass insbesondere die Bilanzkontrolle gestärkt und die Abschlussprüfung weiter reguliert werden müssen, um die Richtigkeit der

⁷⁴ In diesem Sinne auch Böcking/Gros (F. 35), S. 51.

Rechnungslegungsunterlagen von Unternehmen sicherzustellen. Aber auch bei den Aufsichtsstrukturen und den Befugnissen der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) bei der Prüfung von Auslagerungen seitens der Finanzdienstleistungsunternehmen besteht Verbesserungsbedarf.⁷⁵ Indessen traut er sich nicht, die gebotene Abkehr vom schwerfälligen zwei-stufigen System zu vollziehen und allgemeine wert-papierhandelsrechtliche Befugnisse, die ein effizientes und praktikables Eingreifen bei „Gefahr in Verzug“ ermöglichen würden, lässt der Referentenentwurf auch vermissen.

[49] Zu fordern wäre auch eine Reform der Vorgaben, die für eine Nichteinstufung der Wirecard AG als Finanzholding geführt haben. Zurück zum *big picture*: Der Fall zeigt exemplarisch, dass die eingangs zitierten *Dreyling'schen* Schnellboote gut agieren können, aber ein koordinierendes Beiboot, das neben dem Tanker rudert und den Überblick über den Konzern hat, mag einem „Fahren auf Sicht“ in der Aufsicht, wie es durch die hohe normative Spezialisierung derzeit bedingt ist, Abhilfe schaffen.

[50] Die Virologin *Melanie Brinkmann* beschreibt derartige Situationen mit dem sog. „Schweizer Käse-Modell“: Man stelle sich die einzelnen Maßnahmen

gegen eine Pandemie wie hintereinander gelegte Scheiben eines Schweizer Käses vor, von der jede einzelne Löcher hat. Jede einzelne Scheibe (wie AHA-Regeln, eine Tracing App etc.) ist für sich betrachtet imperfekt, weist Löcher auf und bietet einem Virus die Möglichkeit, durch sie hindurch zu schlüpfen. Erst das Hintereinanderlegen mehrerer Scheiben schafft eine undurchdringliche Wand.⁷⁶ Gleiches gilt für die Kriminellen, die sich auch im FinTech-Sektor und sonst auf den Kapitalmärkten tummeln werden: Jede einzelne aufsichts- und strafrechtliche Vorgabe und Maßnahme ist für sich betrachtet imperfekt und wird für sich betrachtet ein neues Wirecard nicht verhindern können. Geboten ist eine Kombination verschiedener Maßnahmen, welche die einzelnen naturgemäß vorhandenen Löcher besser abdichten mag, als dies bisher der Fall ist. Zu denken wäre auch an die Bildung einer Spezial-Eingreiftruppe bestehend aus besonders für die Verfolgung von Wirtschaftskriminalität qualifizierten Mitarbeitern aus BaFin, BKA und Staatsanwaltschaft – die Anforderungen hieran sind jedoch Stoff für einen eigenen (Folge-)Beitrag.

⁷⁵ Referentenentwurf eines Gesetzes zur Stärkung der Finanzmarktintegrität (FISG) (Fn. 50), S. 1

⁷⁶ Twitterpost von ZDF heute vom 3.11.2020, abrufbar unter: <https://beck-link.de/3n672>.

KÜNSTLICHE INTELLIGENZ

RA Dr. Simon Apel/RA Dr. Markus Kaulartz*

Rechtlicher Schutz von Machine Learning-Modellen

Im Machine Learning, einem besonders relevanten Bereich der Künstlichen Intelligenz, wird das Wissen und die (vermeintlich) Intelligenz in sogenannten Modellen gespeichert. Diese sind für Unternehmen von kritischer Bedeutung, ein Abhandenkommen oder unbefugtes Kopieren durch Dritte gefährdet oft die Grundlage ihres Geschäftsmodells. Der Schutz solcher Modelle ist daher essenziell. Der Beitrag analysiert rechtliche Schutzmechanismen und kommt zum Schluss, dass das Urheberrecht, das Datenbank(schutz)recht sowie das Patentrecht unzureichend sind. In der Praxis wesentlich bedeutender ist der Schutz von Künstlicher Intelligenz als Geschäftsgeheimnis unter dem GeschGehG. Der Beitrag leitet hierzu unter dem Stichwort „AI Compliance“ ein und unterbreitet Klauselvorschläge.

* Der Autor *Apel* ist Rechtsanwalt bei SZA Schilling, Zutt & Anschütz in Mannheim und Lehrbeauftragter an der Universität Mannheim und der Friedrich-Alexander-Universität Erlangen. Der Autor *Kaulartz* ist Rechtsanwalt bei CMS Hasche Sigle in München und Gesamtherausgeber der *Recht Digital*. Sämtliche Internetquellen wurden zuletzt am 27.10.2020 abgerufen.

I. Einleitung

[1] Künstliche Intelligenz ist als Oberbegriff¹ schwer greifbar,² fast schon mystisch, jedenfalls hipp und vielleicht gerade deswegen allgegenwärtig. Konkreter werden die Teilbereiche der Künstlichen Intelligenz, worunter das Maschinelle Lernen (Machine Learning³) sicherlich besonders heraussticht. Beim Machine Learning werden Korrelationen in Rohdaten gesucht und das gesammelte Wissen wird in sogenannten „Modellen“ gespeichert. Diese sind wirtschaftlich natürlich umso wertvoller, je höher ihre Qualität ist.⁴ Es stellt sich sodann jedoch die Frage, wie diese Modelle rechtlich geschützt sind und geschützt werden können. Der Beitrag geht auf den urheberrechtlichen, patentrechtlichen und datenbankrechtlichen Schutz ein und kommt zum Schluss, dass Modelle *de lege lata* nicht in den Genuss eines gesetzlichen Schutzes kommen und deswegen in erster Linie durch vertragsrechtliche Mechanismen sowie als geheimes Know-How durch vertragliche, technische und organisatorische Maßnahmen geschützt werden müssen.

II. Technische Einführung in Machine Learning und Modelle

[2] Machine Learning basiert im Kern auf der Überlegung, dass vergleichbare Sachverhalte auf einer vergleichbaren Datenlage beruhen. Ein Bild von einem Menschen am Straßenrand unterscheidet sich anhand bestimmter Merkmale von dem Bild eines Baumes. Verfügt ein Computersystem über diese Merkmale, kann es also, eingebaut etwa in ein autonom fahrendes Fahrzeug, den Menschen vom Baum unterscheiden und damit auch passende Maßnahmen einleiten, wie etwa das Fahrzeug abzubremesen. Nun könnte man diese Merkmale ausdrücklich programmieren,⁵ was sich aber auf Grund der schier unzähligen Merkmale als praktisch nicht durchführbar erweist. Schließlich müsste die Programmierung Menschen aus unterschiedlichen Perspektiven in unterschiedlichen Lichtverhältnissen berücksichtigen. Besser wäre es doch, man könnte einem Computersystem eine große Menge an Fotos mit Menschen und Bäumen vorlegen und das System würde selbstständig Merkmale auf diesen Fotos erkennen, entsprechend klassifizieren und insbesondere weiterlernen.⁶ Ein solches Vorgehen nennt man dann Machine Learning.⁷

[3] Die Daten, mit welchen ein System lernt, werden als Trainingsdaten bezeichnet, dabei handelt es sich um aufbereitete Rohdaten.⁸ Es gibt verschiedene Möglichkeiten, das Trainieren auszugestalten:

1. Trainieren am Beispiel des Supervised Learning

[4] Beim sogenannten Supervised Learning (überwachtes Lernen⁹), einem sehr weit verbreiteten Verfahren,¹⁰

erhält der Machine Learning-Algorithmus bereits klassifizierte Datensätze,¹¹ im Beispiel etwa Fotos von Menschen und von Bäumen, jeweils mit der Information, ob es sich um einen Menschen oder einen Baum handelt. Der Algorithmus versucht sodann, bestimmte Eigenschaften auf den Fotos zu erkennen und ordnet diese entweder dem Menschen oder dem Baum zu. Darunter könnten etwa eine Baumkrone oder zwei Beine fallen. Man bezeichnet die Klassifizierung als Label, während die verschiedenen Eigenschaften Feature genannt werden.¹² Das Label kann dabei in Abhängigkeit von Features dargestellt werden, und deswegen sogar als mathematische Funktion $y = b + w * x$, wobei y das Label (Mensch oder Baum) ist, x das Feature und w und b die Parameter (vektoren).¹³ Die Nutzung von mathematischen Funktionen ist möglich, weil die Features – hier also etwa die Eigenschaften von Mensch und Baum auf einem Bild – durch Zahlen dargestellt werden. Dem Training vorgelagert ist dann mitunter eine Art Übersetzung von Bildern oder Texten in Zahlen. Bei Texten etwa spricht man von einer Vektorisierung von Wörtern, bei der beispielsweise einzelnen Wörtern Zahlen zugewiesen werden, mit denen dann innerhalb der mathematischen Funktion gearbeitet werden kann.¹⁴

[5] Neuronale Netze¹⁵ bringen mehr Komplexität in das Trainieren mittels Machine Learning. Hier werden

1 Zum Begriff *Herberger* NJW 2018, 2825 (2826); *Graf von Westphalen* BB 2020, 1859; Unabhängige Hochrangige Expertengruppe für Künstliche Intelligenz, 2018, Eine Definition der KI: Wichtigste Fähigkeiten und Wissenschaftsgebiete.

2 Siehe nur *Specht* GRUR 2019, 253.

3 Nachfolgend wird der weiteren Verbreitung wegen der englische Begriff verwendet.

4 Die Qualität von Modellen lässt sich, je nach Anwendungsfall, durch verschiedene Metriken bestimmen, wie etwa Genauigkeit oder Robustheit. Siehe zu Beispielen etwa die Erläuterungen unter <https://beck-link.de/4scdd>. Ferner Ebers/Heinze/Krügel/Steinrötter/*Niederée/Nejdl*, Künstliche Intelligenz und Robotik, 2020, § 2, B.I.2.

5 Kaulartz/Braegelmann/*Stiemerling*, Rechtshandbuch Artificial Intelligence und Machine Learning, 2020, Kap. 2.1 Rn. 9 f.

6 Kaulartz/Braegelmann/*Stiemerling*, Rechtshandbuch Artificial Intelligence und Machine Learning, Kapitel 2.1 Rn. 11 ff., 27; Ebers/Heinze/Krügel/Steinrötter/*Niederée/Nejdl*, Künstliche Intelligenz und Robotik, § 2, B.I.1; ferner mit mathematischem Einstieg <https://beck-link.de/pek4> f.

7 Für eine einfache Einführung mit Beispielen siehe *Rocca*, A simple introduction to Machine Learning, 2019, abrufbar unter: <https://beck-link.de/dr2ne>.

8 *Hacker* GRUR 2020, 1025 (1026).

9 *Stiemerling* CR 2015, 762 (763); *Soni*, Supervised vs. Unsupervised Learning, abrufbar unter: <https://beck-link.de/pen7p>.

10 95 % aller Verfahren, zitiert bei *Armour/Eidenmüller* ZHR 183 (2019), 169 (174).

11 *Bilski/Schmid* NJOZ 2019, 657; *Bernhardt* NZKart 2019, 314.

12 Zur Terminologie Kaulartz/Braegelmann/*Kaulartz*, Rechtshandbuch Artificial Intelligence und Machine Learning, Kap. 2.2 Rn. 3 ff.; zu Beispielen siehe <https://beck-link.de/baa3h>.

13 Vgl. näher Kaulartz/Braegelmann/*Kaulartz*, Rechtshandbuch Artificial Intelligence und Machine Learning, Kap. 2.2.

14 Näher dazu etwa *Karani*, Introduction to Word Embedding and Word2Vec, 2018, abrufbar unter: <https://beck-link.de/4dmv2>.

15 Vgl. näher Kaulartz/Braegelmann/*Stiemerling*, Rechtshandbuch Artificial Intelligence und Machine Learning, Kap. 2.1 Rn. 21 ff.; Ebers/Heinze/Krügel/Steinrötter/*Niederée/Nejdl*, Künstliche Intelligenz und Robotik, § 2, B.III.

verschiedene der oben beschriebenen Verfahren in Form von Neuronen und Synapsen (die Terminologie lehnt sich an jene zum menschlichen Gehirn an) hintereinandergeschaltet.¹⁶ Das Prinzip im Kern bleibt bestehen, durch die Kombination der verschiedenen Neuronen durch unterschiedlich gewichtete Synapsen steigt die Komplexität aber sehr an.

[6] Während des Trainingsprozesses versucht der Algorithmus, die Parameter dieser Funktion zu ermitteln. Dies geschieht letztlich durch Ausprobieren, wobei sich in der Praxis verschiedene Verfahren etabliert haben, um den immensen Rechenaufwand zu reduzieren.¹⁷ Der Algorithmus arbeitet solange, bis seine Vorhersage, also das Ergebnis der mathematischen Funktion, nicht mehr näher an die in den Trainingsdaten bereits vorhandene Klassifizierung heranreichen kann (man spricht von *Convergence*). Die Parameter w und b werden typischerweise als Zahlenvektor gespeichert, im Kontext von KI spricht man hier von einem Modell.

[7] Auf der Grundlage eines Modells können dann unbekannte Sachverhalte klassifiziert werden. Mathematisch ausgedrückt: Das Modell gibt einen Wert y aus für gegebene Features x anhand der Parameter (also des Modells) w und b . Wichtig dabei ist, dass Machine Learning probabilistisch, nicht deterministisch arbeitet. Auf der Grundlage eines Modells können nur Wahrscheinlichkeitswerte berechnet (*Prediction*), jedoch keine sicheren Aussagen getroffen werden. Ein KI-System kann also die Aussage treffen „das ist zu 98 % ein Baum“. Es ist sodann Aufgabe der Entwickler, diese Wahrscheinlichkeitswerte in Entscheidungen zu übersetzen, unter welchen Voraussetzungen das Fahrzeug etwa bremst (*Thresholding*¹⁸). Vor diesem Hintergrund kann eine KI keine falschen oder richtigen Ergebnisse liefern. Eine KI kann nur schlecht trainiert worden sein, etwa mit ungeeigneten Fotos, falsch klassifizierten Trainingsdaten oder ungenügender Parametrisierung.

[8] Das Trainieren von Modellen ist ein Prozess, der eigentlich kein Ende kennt. Jeder neue Satz an Trainingsdaten hat das Potential, die Parameter des Modells zu verändern und die Grundlage der Wahrscheinlichkeitsberechnung damit zu verbessern. Deswegen sind KI-Unternehmen auch daran interessiert, ihre Modelle auf Grundlage der ihnen bereitgestellten Daten stets weiter zu trainieren (zum Vorschlag einer Klausel zum Trainieren mit Trainingsdaten eines Vertragspartners siehe Abschnitt VI.2.). Und darum ist es auch verständlich, weswegen Modelle für KI-Unternehmen so wertvoll sind: In ihnen steckt das Destillat unzähliger Trainings, was gerade bei vielen (*Sample Size*¹⁹) und qualitativ hochwertigen Trainingsdaten von besonders großer Bedeutung ist.

[9] In der Praxis sind Modelle natürlich deutlich komplexer als in diesem einfachen Beispiel dargelegt. Dies liegt daran, dass es viele verschiedene Features (also x_1 bis x_n) geben kann, und damit entsprechend viele Parameter (also w_1 bis w_n). Deswegen ist auch das Auffinden der „richtigen“ Parameter sehr ressourcenintensiv und von Menschenhand nicht zu leisten. Denn je mehr Features anhand von Trainingsdaten ausgemacht werden, desto mehr mögliche Muster und Korrelationen gibt es zwischen diesen Features, und desto länger muss ein Algorithmus arbeiten, um passende Parameter zu finden.²⁰

[10] Entsprechend komplex sind solche Modelle, sodass sie von außen nicht mehr nachzuvollziehen, geschweige denn erklärbar sind. Hier verbirgt sich eine für die Praxis große Herausforderung, die auch unter dem Stichwort *Black Box* bekannt ist, und deren Lösungen man unter dem wissenschaftlichen Teilgebiet *Explainable AI* diskutiert.²¹

2. Unsupervised Learning

[11] Neben dem Supervised Learning gibt es noch andere Methoden, um Modelle zu trainieren. Beim Unsupervised Learning (unüberwachtes Lernen²²) etwa erhält der Algorithmus gerade keine Informationen zur Klassifizierung von Daten.²³ Er weiß im Beispiel also nicht, ob das Foto einen Baum oder einen Menschen zeigt. Der Algorithmus versucht vielmehr selbstständig, Labels zu identifizieren (die Variable y der mathematischen Funktion ist also unbekannt im Gegensatz zum Supervised Learning). Daten werden anhand eines Ähnlichkeitsmaßes in Cluster geteilt, sodass Aussagen wie „wer Produkt A kauft, kauft auch Produkt B“ durch den Algorithmus herausgearbeitet werden können. Das Clustering übernimmt der Algorithmus, was das Unsupervised Learning vom Supervised Learning unterscheidet. Unsupervised Learning kann mit Echtdateien arbeiten und kommt daher etwa bei der Anomalieerkennung (*Anomaly Detection*²⁴), Betrugserkennung (*Fraud Detection*²⁵) oder in Webshops bei Produktvorschlägen zum Einsatz.

¹⁶ Söbbing, Fundamentale Rechtsfragen zur künstlichen Intelligenz (AI Law), 2019, 31 ff.

¹⁷ Wie z. B. der Stochastic Gradient Descent, vgl. Srinivasan, Stochastic Gradient Descent — Clearly Explained !, 2019, abrufbar unter: <https://beck-link.de/pzr4c>; ferner <https://beck-link.de/kf3fd>.

¹⁸ Näher <https://beck-link.de/7b3ts>.

¹⁹ Mitsa, How Do You Know You Have Enough Training Data?, abrufbar unter: <https://beck-link.de/bdxe2>.

²⁰ Zum Ausprobieren, welche Parameter das Lernen beeinflussen, sei die Simulation unter <https://beck-link.de/ys4md> empfohlen.

²¹ Kaulartz/Braegelmann/Körner, Rechtshandbuch Artificial Intelligence und Machine Learning, Kap. 2.4.

²² Stiemerling CR 2015, 762 (763); Soni (Fn. 9).

²³ Bilski/Schmid NJOZ 2019, 657 (658); Bernhardt NZKart 2019, 314.

²⁴ Bajaj, Unsupervised Learning For Anomaly Detection, 2020, abrufbar unter: <https://beck-link.de/8nrh7>.

²⁵ Meazzini, Fraud detection — Unsupervised Anomaly Detection, 2020, abrufbar unter: <https://beck-link.de/7nrt6>.

[12] Unsupervised Learning dient damit der Wissensgenerierung aus großen Datenmengen, Supervised Learning dem Vorhersagen von Werten.

III. Schutz nach dem UrhG

1. Vorbemerkung

[13] Da die Verwendung von Modellen stets die Nutzung von Computern voraussetzt, ist es naheliegend,²⁶ bei der Suche nach gesetzlichen Schutzmöglichkeiten für Modelle beim Urheberrecht anzusetzen:²⁷ Computerprogramme sind bereits seit Jahrzehnten als Werkkategorie im Urheberrecht anerkannt.²⁸ Was die Trainingsdaten angeht, steht ebenfalls ein *prima facie* ausichtsreiches Schutzregime als Datenbank zur Verfügung.²⁹ Allerdings zeigt ein näherer Blick, dass dieser Schutz regelmäßig nicht eingreift, da die entsprechenden Schutzvoraussetzungen durch Modelle und die von ihnen im Rahmen des Trainingsprozesses „angereicherten“ Daten regelmäßig nicht oder zumindest nicht mit der für die Praxis erforderlichen Sicherheit erfüllt sind.

2. Schutz als Computerprogramm

[14] Der Begriff des Computerprogramms wird in §§ 2 I Nr. 1, 69 a UrhG nicht legal definiert. Gemeinhin wird hierunter aber „ein Satz von Anweisungen an ein informationsverarbeitendes Gerät und an den mit diesem Gerät arbeitenden Menschen zur Erzielung eines Ergebnisses“³⁰ verstanden.³¹ Bildlich gesprochen geht es also um ein Paket von Befehlen, die ein Computer versteht und ausführt. Irrelevant ist, in welcher Form das Computerprogramm niedergelegt wird (etwa Art der Programmiersprache, Objekt- oder Quellcode). Voraussetzung ist allerdings wie bei allen urheberrechtlichen Werkarten (§ 2 II UrhG), dass das Computerprogramm nach den allgemeinen Maßstäben ein Minimum an Schöpfungshöhe aufweist, also vom menschlichen Urheber³² hinreichend individuell geprägt worden ist.³³

[15] Bereits hieraus folgt, dass nicht jede Form von informationstechnisch verarbeitbarer Information urheberrechtlich als Computerprogramm geschützt ist: Alle Elemente,³⁴ die nicht individuell durch einen menschlichen Urheber geprägt worden sind oder werden können, sind nicht schutzfähig.

[16] Hierzu gehören etwa nach allgemeiner Auffassung „allgemeine Prinzipien mathematischer Logik“,³⁵ aber grundsätzlich³⁶ auch die Algorithmen, die der Computer – etwa im Rahmen des Trainings des Modells – ausführt.³⁷ Diese bewirken letztlich nur den Ablauf eines technischen Vorgangs, der als solches nicht individuell ist. Ebenfalls nicht schutzfähig sind alle Kom-

ponenten eines Modells, die zwar bei unbefangener Betrachtung individuell anmuten, aber eben automatisiert³⁸ von der Maschine und nicht von einem Menschen erzeugt wurden.³⁹

[17] Dies alles schließt selbstverständlich nicht aus, dass die konkrete Formulierung eines Modells oder die spezifische Anordnung der in ihm enthaltenen Algorithmen („innere Struktur“)⁴⁰ bei hinreichender Schöpfungshöhe als Computerprogramm urheberrechtlich schutzfähig sein könnte.⁴¹ Dies ist aber für den Ersteller

²⁶ Vgl. auch *Hacker* GRUR 2020, 1025 (1031).

²⁷ Eingehend hierzu Kaulartz/Braegelmann/Nägele/Apel, *Rechtshandbuch Artificial Intelligence und Machine Learning*, Kap. 7.1; dieser Abschnitt III. basiert auf den dortigen Ausführungen.

²⁸ Ursprünglich als Unterkategorie des Sprachwerks (in Deutschland § 2 I Nr. 1 UrhG), vgl. nur *BGH* GRUR 1985, 1041 – Inkasso-Programm; *Schack*, *Urheber- und Urhebervertragsrecht*, 9. Aufl. 2019, § 9 Rn. 207, später dann als eigene Werkkategorie, Computerprogramme-RL 91/250/EWG (in Deutschland umgesetzt in §§ 69 a ff. UrhG); s. auch Art. 10 I TRIPS und Art. 4 WCT.

²⁹ Und zwar einerseits als urheberrechtlicher Schutz in § 4 UrhG (Datenbankwerk), andererseits als Leistungsschutz, §§ 87 a ff. UrhG; zum kategorialen Unterschied zwischen Urheber- und Leistungsschutzrecht (en) s. nur *Wegmann*, *Der Rechtsgedanke der freien Benutzung des § 24 UrhG und die verwandten Schutzrechte*, 2013, S. 147 ff. – Zum (noch) weniger erfolversprechenden Schutz über § 2 I Nr. 7 (Darstellungen wissenschaftlicher oder technischer Art) UrhG *Hacker* GRUR 2020, 1025 (1027 f.).

³⁰ Schon hieraus folgt, dass (grafische) Benutzeroberflächen nicht als Computerprogramm schutzfähig sind; sie können ggf. selbstverständlich ein Werk der angewandten Kunst (§ 2 I Nr. 4 UrhG) darstellen, vgl. m. w. N. *Schack*, *Urheber- und Urhebervertragsrecht*, § 9 Rn. 209; hierfür müssen sie nur zumindest im Sinne der "kleinen Münze" individuell sein, vgl. *BGH* GRUR 2014, 175 – Geburtstagszug (unter Aufgabe der höheren Anforderungen an die Individualität für einen Urheberrechtsschutz bei Werken der angewandten Kunst).

³¹ *KG Berlin* CR 2010, 424 (425); *OLG Hamburg* CR 1998, 332 (333 f.).

³² Im Kontext des urheberrechtlichen Schutzes von den in neuronalen Netzen enthaltenen Steuerungsbefehlen als Computerprogramm besonders betont von *Ehinger/Stiemerling* CR 2018, 761 (Rn. 43 f.); vgl. auch *Schricker/Loewenheim/ders./Leistner*, *Urheberrecht*, 6. Aufl. 2020, § 2 Rn. 38 m. w. N.; in *Dreier/Hilty/Pfeifer*, *Festschrift 50 Jahre Urheberrechtsgesetz (UrhG)*, 2015, 251 f.

³³ § 69 a III 2 UrhG; *Schack*, *Urheber- und Urhebervertragsrecht*, § 9 Rn. 208.

³⁴ Für den Schutz von Werkteilen gelten dieselben Anforderungen wie für den Schutz des Gesamtwerks, sodass diese selbst nur als Werk schutzfähig sind, wenn sie auch selbst hinreichend individuell durch den menschlichen Urheber geprägt wurden; das Urheberrecht ist insoweit *modular*, weil Werke letztlich aus Modulen schutzfähiger Werkteile bestehen, die ihrerseits aus gemeinfreien Elementen zusammengesetzt sind, vgl. *Apel* in *Festschrift für Martin Vogel zum siebzigsten Geburtstag*, 2017, 205 (212 f.).

³⁵ *Schricker/Loewenheim/ders./Spindler*, *Urheberrecht*, § 69 a Rn. 12.

³⁶ Vgl. aber offener *KG* CR 2010, 424 (425); *Lewke* InTeR 2017, 207 (214).

³⁷ *Schricker/Loewenheim/ders./Spindler*, *Urheberrecht*, § 69 a Rn. 12.

³⁸ Abweichend der Ansatz des britischen Urheberrechts, das bei computer-generierten Werken als potenziell schutzfähig anerkennt, Art. 9, 178 Copyright Act, vgl. *Bently/Sherman/Gangjeel/Johnson*, *Intellectual Property Law*, 5. Aufl. 2018, 3.7.8 (S. 117 f.); *Peifer* in *Urheberrecht! Festschrift für Michel M. Walter zum 80. Geburtstag*, 2018, 222 (227 f.).

³⁹ Zur parallelen Problematik im patentrechtlichen Kontext etwa *Claessen* IPRB 2020, 38; *Stierle* GRUR-Int 2020, 918.

⁴⁰ Vgl. nur *KG Berlin* CR 2010, 424 (425); *Wandtke/Bullinger/Grützmacher*, *PK-Urheberrecht*, 5. Aufl. 2018, § 69 a Rn. 23 m. w. N.

⁴¹ Vgl. nur *Söbbing*, *Fundamentale Rechtsfragen zur künstlichen Intelligenz (AI Law)*, 2019, 11 ff.; *Ehinger/Stiemerling* CR 2018, 761 (Rn. 43 f., 66) sowie *Bischoff/Intveen* ITRB 2019, 134 (136); *Hartmann/Prinz* WRP 2018, 1431 (Rn. 29 ff.); zum denkbaren, aber noch nicht praktisch verprobten Schutz neuronaler Netze als Computerprogramm *Hartmann/Prinz* DSRITB 2018, 769 (783 ff.).

von Modellen insoweit nicht befriedigend, als der eigentliche „Witz“ – ihre technische Funktionalität – urheberrechtlich gemeinfrei bleibt. Auch dies ist aber keine Besonderheit, sondern Ausfluss des allgemeinen urheberrechtlichen Prinzips, das bloße Ideen oder Konzepte als solche nicht urheberrechtlich schutzfähig sind.⁴²

[18] Auch wenn es damit im Einzelfall gelingen mag, ein Modell so zu „komponieren“, dass ein urheberrechtlicher Schutz als Computerprogramm greift, bleibt dieser für die Praxis einstweilen eine unsichere und insbesondere in seinem Schutzbereich unklare Option.

3. Schutz als Datenbank

[19] Nach der Legaldefinition des § 87a I 1 UrhG ist eine Datenbank „eine Sammlung von Werken, Daten oder anderen unabhängigen Elementen, die systematisch oder methodisch angeordnet und einzeln mit Hilfe elektronischer Mittel oder in anderer Weise zugänglich sind.“ „Unabhängig“ meint hier, dass die einzelnen Elemente voneinander getrennt werden können, ohne dass hierdurch der Wert ihres Inhalts beeinträchtigt wird.⁴³ Rohdaten und bloße „Datenhaufen“ können demnach mangels systematischer oder methodischer Anordnung nicht als Datenbank geschützt sein.⁴⁴

[20] Das UrhG schützt Datenbanken auf zwei voneinander unabhängigen Ebenen (siehe Abschnitt III.1.) potenziell durch ein Urheberrecht am Datenbankwerk (§§ 2 II 4 UrhG) und ein Leistungsschutzrecht an der Datenbank, wenn und soweit „die Beschaffung, Überprüfung oder Darstellung“ der enthaltenen Elemente „eine nach Art oder Umfang wesentliche Investition erfordert“ (§ 87a I UrhG). Im erstgenannten Fall ist Schutzgegenstand demnach das Datenbankwerk selbst, wenn es gerade durch die Auswahl oder Anordnung der Elemente hinreichend individuell geprägt ist.⁴⁵ Inhaber des Rechts ist in diesem Fall der Urheber.⁴⁶ Im zweiten Fall ist Schutzgegenstand die Investition in die Herstellung der Datenbank,⁴⁷ Inhaber des Leistungsschutzrechts ist dann derjenige, der diese tätigt – gleich, ob natürliche Person oder nicht.⁴⁸ Das Leistungsschutzrecht ist demnach auch frei übertragbar.

[21] Im Kontext des Rechtsschutzes für Modelle ist in erster Linie der Leistungsschutz für die Herstellung einer Datenbank interessant, da er das Problem der Schöpfungshöhe und der menschlichen Erstellung vermeidet (siehe Abschnitt III.2.). Allerdings treten auch hier zahlreiche Schwierigkeiten auf, die den Wert dieser Schutzoption für die Praxis mindern.

[22] Dies beginnt schon damit, dass die in der Datenbank enthaltenen Daten selbst nicht durch das Leistungsschutzrecht geschützt werden.⁴⁹ Deren unabhängige

Gewinnung durch einen Dritten bleibt also möglich.⁵⁰ Weiter enthält das Leistungsschutzrecht eine *de minimis*-Grenze,⁵¹ sodass es nur Schutz gegen die unbefugte Verwertung eines „nach Art oder Umfang wesentlichen Teil[s] der Datenbank“ bietet (§ 87 b I 1 UrhG).

[23] Weiter ist unklar, wie genau die hinreichende Wesentlichkeit der für den Leistungsschutz erforderlichen Investition in die Datenbank festzustellen ist. Insbesondere ist insoweit gesichert, dass der Aufwand für die *Erzeugung* der in der Datenbank enthaltenen Daten wegen des eindeutigen Gesetzeswortlauts hierfür nicht maßgeblich ist und daher außer Betracht bleiben muss.⁵² Da Modelle im Laufe des Trainingsprozesses die eingespeisten Daten „anreichern“ und in diesem Sinne erst erzeugen, ist die Abgrenzung zwischen dem hierfür anfallenden, nicht maßgeblichen Aufwand und dem berücksichtigungsfähigen Aufwand für die Beschaffung, Überprüfung oder Darstellung der in der Datenbank enthaltenen Daten in diesem Fall besonders mit Unsicherheiten belastet.⁵³ Zwar gibt es im Schrifttum auch optimistischere Stimmen hierzu, die argumentieren, dass in diesen Fällen die Monopolisierung der erzeugten Daten „an sich“ nicht drohe, da grundsätzlich entsprechende „Trainings“ von jedermann aufgesetzt werden können.⁵⁴ Ob sich diese durchsetzen werden, scheint aber derzeit offen.

[24] Fraglich ist auch, wann eine Investition im Sinne des Gesetzes „wesentlich“ ist. Die höchstrichterliche Rechtsprechung fordert hierfür großzügig, dass nicht lediglich ganz unbedeutende Aufwendungen getroffen wurden.⁵⁵ Instanzgerichte haben auch schon etwas

42 Kaulartz/Braegelmann/Nägele/Apel, *Rechtshandbuch Artificial Intelligence und Machine Learning*, Kap. 7.1 Rn. 19 m. w. N.

43 *EuGH* GRUR 2015, 1187 Rn. 17 – Freistaat Bayern/Verlag Esterbauer; vgl. auch *Hacker* GRUR 2020, 1025 (1028 f.).

44 Statt aller in Sassenberg/Faber/Sattler, *Rechtshandbuch Industrie 4.0 und Internet of Things*, 2. Aufl. 2020, Kap. 2, Rn. 33.

45 Vgl. *EuGH* GRUR 2012, 368 Rn. 35 ff. – Football Dataco/Yahoo.

46 §§ 7, 11, 29 I UrhG.

47 *OLG Hamburg* GRUR 2000, 319 (329), *Schack*, Urheber- und Urhebervertragsrecht, § 20 Rn. 744.

48 Fromm/Nordemann/Czychowski, *Urheberrecht*, 12. Aufl. 2018, § 87 a Rn. 25 ff. m. w. N.

49 Vgl. Art. 1 III Datenbank-RL 96/9/EG; Schrickler/Loewenheim/*Leistner*, *Urheberrecht*, § 4 UrhG Rn. 85 (zum entsprechenden Problem beim Datenbankwerk).

50 Dies gilt freilich auch, wenn man die Kodierung der Daten über § 85 UrhG (Tondatei) schutzfähig stellt, zu dieser Möglichkeit in Kaulartz/Braegelmann/Nägele/Apel, *Rechtshandbuch Artificial Intelligence und Machine Learning*, Kap. 7.1 Rn. 49 ff.

51 Leistungsschutzrechte sind im Ausgangspunkt *holistisch*, da sie ein konkretes Leistungsergebnis schützen; eine Begrenzung des Teileschutzes bedarf daher einer ausdrücklichen Anordnung durch den Gesetzgeber, näher *Apel* in *Festschrift für Martin Vogel zum siebzigsten Geburtstag*, 205 (212 f.).

52 *EuGH* GRUR 2005, 244 Rn. 31 ff. – BHB-Pferdewetten; *Söbbing* K&R 2019, 164 (167).

53 Vgl. zu diesen Schwierigkeiten allgemein auch Sassenberg/Faber/Sattler, *Rechtshandbuch Industrie 4.0 und Internet of Things*, Kap. 2 Rn. 35 ff.

54 *Söbbing*, *Fundamentale Rechtsfragen zur künstlichen Intelligenz (AI Law)*, S. 38; *Schmidt/Zech* CR 2017, 417 (421 f.); vgl. auch *Hacker* GRUR 2020, 1025 (1028).

55 *BGH* GRUR 2011, 724 Rn. 23 – Zweite Zahnarztmeinung II.

strenger entschieden und erhebliche Aufwendungen in qualitativer oder quantitativer Hinsicht gefordert.⁵⁶ Je nachdem, wie die Daten, die das Modell ausgewertet bzw. generiert, zusammengetragen und geordnet wurden, kann also auch dieser Punkt problematisch sein: Eine einfache Abfrage öffentlich zugänglicher Datenbanken (Beschaffung) dürfte z. B. keinen hinreichenden Aufwand generieren, um das Erzeugnis in den Bereich des datenbankrechtlichen Leistungsschutzes zu bringen.

[25] Die im Modell enthaltenen Elemente können außerdem gerade nicht mehr unabhängig voneinander verwendet werden, sondern erhalten ihren Wert erst durch die Inbezugsetzung miteinander, weswegen ein weiteres Element einer Datenbank nicht vorliegt.⁵⁷

4. Zwischenergebnis

[26] Für die Praxis bleiben also *de lege lata* für den urheberrechtlichen Schutz von Modellen zu viele Fragezeichen, auch wenn dieser unter den gezeigten Ansatzpunkten nicht unmöglich ist. Zwar sollten daher urheberrechtliche Ansatzpunkte in jedem Einzelfall sorgfältig geprüft werden, um sie – ggf. auch schon bei der Designentscheidung für die Gestaltung des Modells – so einzubeziehen, dass ein urheberrechtlicher oder (vielsprechender) Leistungsschutz gut vertretbar ist. Allein auf einen urheberrechtlichen Schutz wird man sich aber wohl selten verlassen wollen.

IV. Patentrechtlicher Schutz

[27] Auch das Patentrecht vermag für den immaterialgüterrechtlichen Schutz von Modellen *de lege lata* wenig auszurichten.⁵⁸

1. Hauptproblem: Technizität

[28] Grund hierfür ist, dass der Patentschutz von Computerprogrammen (vom Gesetz etwas umständlich als „Programme für Datenverarbeitungsanlagen“ bezeichnet) *de lege lata* nach § 1 III Nr. 1, 3 PatG ausgeschlossen ist.⁵⁹ Wie auch sonst bei Computerprogrammen ist ein Patentschutz also nur denkbar, wenn über die Verarbeitung des betreffenden Programms durch einen Computer hinaus eine Technizität in dem Sinne hinzutritt, dass das betreffende Computerprogramm (allein oder in Zusammenspiel mit einer weiteren Anlage) neben der Datenverarbeitung einen weiteren technischen Effekt erzeugt oder ein technisches Problem löst (computerimplementierte Erfindung).⁶⁰ Nicht patentierbar ist daher die mathematische Regel, nach der ein Modell arbeitet (Algorithmus)⁶¹ und freilich auch nicht das Computerprogramm als solches, welches das Modell operabel macht.⁶²

[29] Hinsichtlich eines Modells könnte man eine solche Technizität grundsätzlich darin sehen, wie diese Daten konkret gestaltet und verarbeitet werden, um einen bestimmten Effekt zu erreichen.⁶³ Die Praxis der Ämter gibt insoweit aber derzeit wenig Grund zum Optimismus aus Sicht des Schutzsuchenden.⁶⁴

[30] Ein weiterer Ansatz könnte ein mittelbarer Schutz über ein Verfahrenspatent sein: Wenn das Verfahren, das die Daten, die das Modell verwendet oder erzeugt, seinerseits nach § 9 II Nr. 2 PatG geschützt ist, kann dieser Schutz die ausgegebenen Daten erfassen, wenn und soweit die sachlichen und technischen Eigenschaften für die erzeugten Daten „prägend“ sind.⁶⁵

[31] Zu den geschilderten Schwierigkeiten treten freilich die weiteren patentrechtlichen Schutzvoraussetzungen hinzu (Neuheit, erfinderische Tätigkeit durch einen Menschen⁶⁶), die ebenfalls erst einmal erfüllt sein müssen.

2. Zwischenergebnis

[32] Für das Patentrecht ergibt sich also ebenfalls ein eher ernüchternder Befund für den immaterialgüterrechtlichen Schutz von Modellen: Nicht gänzlich ausgeschlossen, aber großteils eher hypothetisch und jedenfalls mit großer praktischer Unsicherheit behaftet.

V. Know-How-Schutz

[33] Der Schutz geheimen Know-Hows – oder (Geschäfts-)Geheimnisschutz – hat sich bereits seit geraumer Zeit zu einem in der Praxis bedeutsamen Rechts-

⁵⁶ Etwa *LG Köln* ZUM-RD 2000, 304 (306); näher zum Ganzen etwa *Schack*, Urheber- und Urhebervertragsrecht, § 20 Rn. 745.

⁵⁷ Skeptisch daher mit Recht *Ehring/Stiemerling* CR 2018, 761 (Rn. 63 ff., 61) mit Verweis auf *EuGH* v. 29.10.2015 – Rs. C-490/14; vgl. auch *Hacker* GRUR 2020, 1025 (1028).

⁵⁸ Vgl. etwa *BPatG* BeckRS 2015, 13810.

⁵⁹ S. nur Kaulartz/Braegelmann/*Tochtermann*, Rechtshandbuch Artificial Intelligence und Machine Learning, Kap. 7.3 Rn. 7 ff.

⁶⁰ Vgl. nur *BGH* GRUR 1990, 430 (431 f.) – Tauchcomputer; Haedicke/Timmann/*Nack*, Handbuch des Patentrechts, 2. Aufl. 2020, § 2 Rn. 248 ff.; Sassenberg/Faber/*Sattler*, Rechtshandbuch Industrie 4.0 und Internet of Things, Kap. 2 Rn. 23; *Ménière/Pihlajaama* GRUR 2019, 332 (zur Praxis des EPA im Bereich KI).

⁶¹ *Söbbing*, Fundamentale Rechtsfragen zur künstlichen Intelligenz (AI Law), S. 35; *Söbbing* K&R 2019, 164 (166); nur i. E. auch *Scheja* CR 2018, 485 Rn. 7.

⁶² Vgl. nur Kaulartz/Braegelmann/*Tochtermann*, Rechtshandbuch Artificial Intelligence und Machine Learning, Kap. 7.3 Rn. 8.

⁶³ Offen hierfür Kaulartz/Braegelmann/*Tochtermann*, Rechtshandbuch Artificial Intelligence und Machine Learning, Kap. 7.3 Rn. 13 unter Verweis u. a. auf *Hauck/Cevc* ZGE 2019, 135 (151).

⁶⁴ Näher Kaulartz/Braegelmann/*Tochtermann*, Rechtshandbuch Artificial Intelligence und Machine Learning, Kap. 7.3 Rn. 14.

⁶⁵ Vgl. nur *BGH* GRUR 2012, 1230 Rn. 21 ff. – MPEG-2-Videosignalcodierung; Sassenberg/Faber/*Sattler*, Rechtshandbuch Industrie 4.0 und Internet of Things, Kap. 2 Rn. 21; *Hettmank/Lauber-Rönsberg* GRUR 2018, 574 (577).

⁶⁶ Besonders kritisch hierzu *de lege ferenda* *Konertz/Schönhof* ZGE 2018, 380 (411). S. auch *Stierle* GRUR-Int 2020, 918.

gebiet entwickelt.⁶⁷ In den vergangenen Monaten hat er auch die seiner Bedeutung gebührende gesetzliche Ausgestaltung erfahren: Basierend auf der Geheimnisschutzrichtlinie⁶⁸ regelt das Geheimnisschutzgesetz (GeschGehG) seit seinem Inkrafttreten am 26.4.2019, unter welchen Voraussetzungen ein Geschäftsgeheimnis vorliegt und wie Geschäftsgeheimnisse geschützt werden, etwa durch zivilrechtliche Handlungsverbote (§ 4 GeschGehG) und flankierende Strafvorschriften (§ 23 GeschGehG).⁶⁹ Der Schutz von Geschäftsgeheimnissen erlangt im Kontext von Modellen eine ganz besonders große Relevanz,⁷⁰ da *de lege lata* keine andere hinreichend verlässliche Möglichkeit zu bestehen scheint, um Modelle mit Mitteln des Rechts zu schützen (siehe die Abschnitte III. und IV.). Zwar ist auch der Schutz geheimen Know-Hows nach dem GeschGehG kein „Selbstläufer“ und er ist sehr fragil (Verlust durch Offenbarung des Geheimnisses, kein absolutes Recht des Geheimnissinhabers),⁷¹ aber er ist insoweit dankbar, als dass er an Inhalt und erst recht Genese oder Funktionsweise des betreffenden Geheimnisses keine nennenswerten Anforderungen stellt. So kann etwa ein ansonsten nicht schutzfähiger Algorithmus ohne Weiteres Gegenstand eines Geschäftsgeheimnisses sein.⁷²

1. Schutzvoraussetzungen

[34] Um in den Genuss des Schutzes des GeschGehG zu kommen, muss ein Modell zunächst als Geschäftsgeheimnis qualifiziert werden. Im Gegensatz zur früheren Rechtslage unter §§ 17 f. UWG⁷³ genügt dazu nicht mehr nur ein subjektiver Geheimhaltungswille, eine fehlende Offenkundigkeit⁷⁴ und ein Geheimhaltungsinteresse.⁷⁵ Hinzu kommen nunmehr neben einem erforderlichen berechtigten Interesse (§ 2 I lit. c GeschGehG) insbesondere angemessene Geheimhaltungsmaßnahmen (§ 2 I lit. b GeschGehG), die letztlich den Geheimhaltungswillen objektiv dokumentieren.⁷⁶ Zudem muss das Geschäftsgeheimnis gerade wegen seiner Geheimheit einen wirtschaftlichen Wert haben (§ 2 I lit. a GeschGehG),⁷⁷ was im Kontext der Künstlichen Intelligenz freilich in aller Regel gegeben sein wird.⁷⁸

2. Was sind angemessene Schutzmaßnahmen?

[35] In der Praxis steht und fällt der Geschäftsgeheimnisschutz damit mit den Schutzmaßnahmen, die der Geheimnissinhaber trifft: Sind diese nicht angemessen, kann er keinen Schutz des Geheimnisses mehr beanspruchen und dieser ist endgültig *perdu*.

[36] Wie Geheimhaltungsmaßnahmen konkret auszusehen haben, überlässt der Gesetzgeber dem Inhaber des Geschäftsgeheimnisses, erleichtert es ihm aber durch die Einschränkung der Einzelfallbezogenheit, die sich durch das Adjektiv „angemessen“ ausdrückt. Nach der

Gesetzesbegründung sind maßgeblich neben dem Wert des Geschäftsgeheimnisses⁷⁹ „dessen Entwicklungskosten, die Natur der Informationen, die Bedeutung für das Unternehmen, die Größe des Unternehmens, die üblichen Geheimhaltungsmaßnahmen in dem Unternehmen, die Art der Kennzeichnung der Informationen und vereinbarte vertragliche Regelungen mit Arbeitnehmern und Geschäftspartnern“⁸⁰ und sicherlich auch das Gefährdungspotential.⁸¹ Eine Praxis und insbesondere Rechtsprechung wird sich dazu noch finden müssen, sinnvoll ist jedenfalls eine Art „wirtschaftlich vertretbares, aber dennoch geschlossenes Schutzkonzept“,⁸² das auch konkrete Schutzmaßnahmen sowohl technischer als auch organisatorischer und rechtlicher⁸³ Na-

⁶⁷ S. nur eingehend zur Entwicklung *Brammsen*, Lauterkeitsstrafrecht, 3. Aufl. 2020, Vor §§ 17–19 UWG Rn. 7 ff. m. w. N.

⁶⁸ Richtlinie (EU) 2016/943 des Europäischen Parlaments und des Rates vom 8. Juni 2016 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse) vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung. Zu dieser eingehend die hilfreiche Kommentierung von MüKo-Lauterkeitsrecht/*Namysłowska*, Band 1, 3. Aufl. 2020, B.III; eingehender Überblick etwa bei *Harte-Bavendamm/Ohly/Kalbfus/ders.*, GeschGehG, 2020, Einl. A Rn. 58 ff.; *Brammsen/Apel/ders.*, GeschGehG, 2021, Einl. C Rn. 11 ff. (im Erscheinen).

⁶⁹ Im Überblick zum GeschGehG etwa *Alexander* WRP 2019, 673; *Apel/Walling* DB 2019, 891; *Ohly* GRUR 2019, 441.

⁷⁰ Eingehend *Scheja* CR 2018, 485; knapper zur besonderen Relevanz *Schricker/Loewenheim/Leistner*, Urheberrecht, § 2 Rn. 41 a. a. E.; *Harte-Bavendamm/Ohly/Kalbfus/Ohly*, GeschGehG, Einl. A Rn. 1; *Söbbing*, Fundamentale Rechtsfragen zur künstlichen Intelligenz (AI Law), S. 14 ff., 41.

⁷¹ Vgl. nur *Köhler/Bornkamm/Feddersen/Alexander*, UWG, 38. Aufl. 2020, Vor § 1 GeschGehG Rn. 78; *Hacker* GRUR 2020, 1025 (1032).

⁷² *BGH* MMR 2014, 489 LS 3, Rn. 27 – SCHUFA (allerdings im Kontext eines datenschutzrechtlichen Auskunftsanspruchs vor Inkrafttreten der DSGVO); *Auer-Reinsdorff/Conrad/ders./Schneider*, Handbuch IT- und Datenschutzrecht, 3. Aufl. 2019, § 11 Rn. 108; *Maute/Mackenrodt/Rühlicke*, Recht als Infrastruktur für Innovation, 2019, 9 (21 ff.); *Scheja* CR 2018, 485 Rn. 11 ff.

⁷³ *BGH* NSz 2014, 325 (326); GRUR 2009, 603 (604); BeckOK-UWG/*Kalbfus*, 4. Ed. 29.6.2017, § 17 Rn. 2 ff.; *Brammsen*, Lauterkeitsstrafrecht, § 17 UWG Rn. 9 ff. m. w. N.

⁷⁴ Heute näher definiert in § 2 I lit. a GeschGehG.

⁷⁵ Unklar *Hacker* GRUR 2020, 1025 (1032), der den Schutz von Trainingsdaten nach dem GeschGehG offenbar unabhängig von einem „faktisch-vertraglichen“ Schutz erörtert und mit letzterem auch organisatorische und technische Schutzmaßnahmen meint; beide Schutzebenen sind nach § 2 I Nr. 1 GeschGehG nicht trennbar.

⁷⁶ *Ohly* GRUR 2019, 441 (443) mit Verweis auf *Kalbfus* GRUR-Prax 2017, 391.

⁷⁷ Auch dies ist gegenüber der bisherigen deutschen Rechtslage neu, vgl. hierzu nur *Harte-Bavendamm/Ohly/Kalbfus/Harte-Bavendamm*, GeschGehG § 2 Rn. 36 ff.; *Brammsen/Apel/ders.*, GeschGehG, Einl. C Rn. 31 ff.

⁷⁸ Optimistisch zur Schützbarkeit von Trainingsdaten unter dem GeschGehG auch *Hacker* GRUR 2020, 1025 (1032); *Hessell/Leffler* MMR 2020, 647 (648 ff.); s. auch *Schau* GRUR 2020, 1142.

⁷⁹ Kritisch hierzu aber *Lauck* GRUR 2019, 1132.

⁸⁰ BT-Drs. 19/4724, S. 25.

⁸¹ *Maaßen* GRUR 2019, 352 (358).

⁸² *Kalbfus* GRUR-Prax 2017, 391 (392).

⁸³ Vertragliche Schutzmaßnahmen sind wie stets beim Umgang mit nicht absolut geschützten Rechtsgütern besonders essentiell, s. etwa im datenschutzrechtlichen Kontext nur *Berger* ZGE 2017, 340 (341) („contract is king“); *Specht-Riemenschneider/N. Werry/S. Werry/Röttgen*, Datenrecht in der Digitalisierung, 2020, § 4.2 Rn. 29 ff.; *Sassenberg/Faber/Sattler*, Rechtshandbuch Industrie 4.0 und Internet of Things, Kap. 2 Rn. 107 ff. und im Kontext der künstlichen Intelligenz *Kaulartz/Braegelmann/Schicker*, Rechtshandbuch Artificial Intelligence und Machine Learning, Kap. 7.2 Rn. 3, 32 sowie *Hacker* GRUR 2020, 1025 (1032).

tur verlangt, die zu Nachweiszwecken auch gut dokumentiert sein sollten. Ein optimaler Schutz ist natürlich nicht erforderlich.⁸⁴

3. Vorgehen bei Modellen

[37] Trotz der großen Verunsicherung, die bei der Frage der Angemessenheit von Schutzmaßnahmen unter dem GeschGehG noch herrscht, lassen sich für Modelle bereits erste Hinweise geben:

[38] In technischer Hinsicht ist es empfehlenswert, je nach Bedeutung des Geschäftsgeheimnisses übliche Maßnahmen wie Passwortsicherung, Verschlüsselung, Aufbewahrung an einem sicheren Ort *et cetera* zu berücksichtigen. Dies mag trivial klingen, ist aber gerade bei kleineren Unternehmen oder Startups, die im Bereich der Künstlichen Intelligenz arbeiten, leider nicht selbstverständlich.

[39] In organisatorischer Hinsicht sollte der Geschäftsgeheimnisbestand des Unternehmens erfasst und evaluiert werden; nur so ist sichergestellt, dass wichtige Geschäftsgeheimnisse bekannt sind („Kronjuwelen“) und ein ggf. nach Bedeutung der Geschäftsgeheimnisse gestaffelter und dokumentierter Geschäftsgeheimnisschutz etabliert werden kann. Weiter sollte insbesondere auf Zugangs- und Zugriffsbeschränkungen sowie die regelmäßige Kontrolle von deren Einhaltung geachtet werden. Die Belegschaft des Geheimnisinhabers sollte durch angemessene allgemeine, interne Richtlinien und Anweisungen mit der Bedeutung des Geschäftsgeheimnisschutzes und den für diesen geltenden Regeln und Prozessen im Unternehmen vertraut gemacht und nachhaltig zu deren Einhaltung ermahnt werden (Etablierung einer Geschäftsgeheimnis-Compliance).⁸⁵ Weiter ist zu überwachen, dass diese auch befolgt werden (etwa Einhaltung von Passwort-Richtlinien).

[40] Empfehlenswert ist auch die Durchführung von Überprüfungen von Arbeitnehmern und Dienstleistern, die mit Geschäftsgeheimnissen in Kontakt kommen, und zwar nicht nur vor Beginn eines Arbeitsverhältnisses (Pre-Employment-Screening),⁸⁶ sondern auch bevor sie innerhalb der Organisation erweiterten Zugang zu Geschäftsgeheimnissen erhalten (Rollenwechsel).

[41] Auch bei der Produktvermarktung sollten Aspekte des Geschäftsgeheimnisschutzes mit bedacht werden: So kann es sich etwa anbieten, bei der Vermarktung des Modells eher auf SaaS-Lösungen zu setzen (Black Box), bei dem das Modell und der Datenbestand auf Systemen des Inhabers des Modells laufen und nicht auf Kunden-Infrastrukturen eingebunden werden (White Box): Damit begrenzt man, soweit technisch einschlägig, auch das Risiko eines Reverse Engineering (§ 3 I Nr. 2 GeschGehG)⁸⁷ oder einer

nach dem UrhG erlaubten Dekompilierung (§ 69 e UrhG) zur Aufdeckung der im Modell verkörperten Geschäftsgeheimnisse. Daneben werden sogenannte Membership-Inference-Attacks⁸⁸ und Model-Inversion-Attacks⁸⁹ zum teilweisen Rekonstruieren von Trainingsdaten, mit denen das Modell trainiert worden ist, deutlich erschwert.

[42] Auf der Ebene der rechtlichen Schutzmaßnahmen von nicht zu unterschätzender Bedeutung sind vertragliche Regelungen mit allen relevanten Personen, die bestimmungsgemäß mit dem Modell in Kontakt kommen. Insbesondere Dienstleister und Arbeitnehmer sollten stets ausdrücklich über ihre Geheimhaltungspflichten aufgeklärt und im Rahmen des Arbeitsvertrags auf diese verpflichtet werden. Auch wenn manche Regelungen des GeschGehG nicht zu Lasten dieser Personen abbedungen werden können (insbesondere in AGB),⁹⁰ ist eine wirksame Vertraulichkeitsvereinbarung ein zentraler Baustein für den rechtlichen Schutz von Geschäftsgeheimnissen. Von großer Bedeutung für die Abschreckungswirkung und „Durchschlagskraft“ von Vertraulichkeitsvereinbarung als Schutzmaßnahme i. S. d. GeschGehG zwingend erforderlich sind, wird von der Literatur teilweise abgelehnt,⁹¹ teilweise befürwortet.⁹² Jedenfalls sind sie aber sehr zu empfehlen, weil ein Schaden im Rahmen eines Schadensersatzanspruchs sonst schwer oder gar nicht darzulegen ist.⁹³ Die

⁸⁴ LAG Düsseldorf GRUR-RS 2020, 23408 Rn. 81.

⁸⁵ Vgl. nur *Leister* GRUR-Prax 2020, 145.

⁸⁶ Hierbei sind freilich insbesondere die (engen) datenschutzrechtlichen Grenzen zu beachten, vgl. im Überblick nur *Thüsing/Wurth/Hexel/Hartung*, Social Media im Betrieb, 2. Aufl. 2020, § 3 Rn. 3 ff.; *Schwarz* ZD 2018, 353; von dem *Bussche/Voigt/Voigt/H. Oenning/J. Oenning*, Konzerndatenschutz, 2. Aufl. 2019, Kap. 1 Rn. 45 ff.

⁸⁷ Es ist strittig, ob und inwieweit die Erlaubnis zum Reverse Engineering (§ 3 I Nr. 2 GeschGehG) in AGB wegen § 307 I 1, II Nr. 1 BGB (Abweichung von gesetzlichem Grundgedanken) wirksam abbedungen werden kann, zumindest bei öffentlich verfügbaren Produkten oder Gegenständen ist dies nicht möglich, s. nur *Leister* GRUR-Prax 2019, 175 (176); *Otte-Gräbener/Kutscher-Puis* ZVertriebsR 2019, 288; *Harte-Bavendamm/Ohly/Kalbfus/Ohly*, GeschGehG, § 2 Rn. 25, 27; weitergehend *Apel/Walling* DB 2019, 891 (896).

⁸⁸ *Shokri/Stronati/Congzheng/Shmatikov*, Membership Inference Attacks Against Machine Learning Models, abrufbar unter: <https://beck-link.de/xa4w7>.

⁸⁹ *Veale/Binns/Edwards*, Algorithms that Remember: Model Inversion Attacks and Data Protection Law, abrufbar unter: <https://beck-link.de/4wtyr>.

⁹⁰ Vgl. nur für § 5 GeschGehG (weitergehend) *Apel/Boom* GRUR-Prax 2020, 225.

⁹¹ *Jansen/Hofmann* BB 2020, 259 (264); *Hille* WRP 2020, 824 Rn. 52 ff.; *Drescher* Industrie- und Wirtschaftsspionage in Deutschland, 2019, S. 295 f. m. Fn. 1255.

⁹² *Apel/Walling* DB 2019, 891 (895); *Barth/Corzelius* WRP 2019, 29 Rn. 12; *Kaulartz/Braegelmann/Schicker*, Rechtshandbuch Artificial Intelligence und Machine Learning, Kap. 7.2 Rn. 6; näher zum Streit m. w. N. für beide Seiten *BeckOF*, IT- und Datenrecht/*Apel*, 4. Ed. 2020, 3.5 Anm. 18; *Brammsen/Apel/ders.*, GeschGehG, Einl. C Rn. 49.

⁹³ *Redeker*, IT-Recht, 7. Aufl. 2020, Teil B Rn. 421; vgl. auch *Böhm/Nestler* GRURPrax 2018, 181; zur ökonomischen Analyse von Geschäftsgeheimnissen vor dem Hintergrund des GeschGehG eingehend *Brammsen/Apel/Hille*, GeschGehG, Einl. F Rn. 11 ff.

Rechtsprechung hat sich mit dieser Frage bislang noch nicht explizit auseinandergesetzt, ein erstes arbeitsgerichtliches Urteil scheint eine Vertragsstrafenklausel aber nicht zwingend zu verlangen, um eine Vertraulichkeitsvereinbarung im Sinne des GeschGehG für hinreichend zu halten.⁹⁴

4. Zwischenergebnis

[43] Was den Schutz von KI-Modellen anbelangt, wird man schlussfolgern können, dass diese für das Unternehmen von hoher Bedeutung sind, und verhältnismäßige Geheimhaltungsmaßnahmen daher sowohl in technischer und organisatorischer als auch in rechtlicher Sicht eine gewisse Qualität erreichen müssen. Dies könnte sich etwa in Zugriffsrechten auswirken sowie in Verschlüsselungen. Geschäftspartner, welche Zugriff auf das KI-Modell erhalten, sollten auf die Verschwiegenheit verpflichtet werden (siehe den Klauselvorschlag in Abschnitt VI.3.), und eine solche Verpflichtung sollte – weil der Schaden bei einem Verlust des Modells schwer zu beziffern ist – schon aus Gründen unternehmerischer Vorsicht⁹⁵ jedenfalls auch eine Vertragsstrafenregelung enthalten. Aufgrund der noch fehlenden belastbaren Leitlinien durch die Rechtsprechung dürfte es derzeit ratsam sein, lieber ein „Zuviel“ als ein „Zuwenig“ an Geschäftsgeheimnisschutz zu etablieren.

VI. Klauselvorschläge

[44] Im Zusammenhang mit Modellen gibt es zahlreiche vertragliche Fallkonstellationen. Um der bereits skizzierten großen Bedeutung vertraglicher Schutzmaßnahmen für die Modelle gerecht zu werden (siehe Abschnitt V.), können etwa die nachfolgenden Klauselvorschläge hilfreich sein, die zwar nicht erschöpfend sind, aber eine Auswahl von wichtigen Regelungspunkten abdecken:

1. Vertraulichkeit

[45] *Vorbemerkung:* Die Verpflichtung zur Vertraulichkeit ist der Grundstein des vertraglichen Geschäftsgeheimnisschutzes. Um ihn hinreichend durchschlagskräftig zu gestalten, ist die Vereinbarung einer Vertragsstrafe für den Verletzungsfall zumindest dringend zu empfehlen. Diese kann aber auch im Wege des aus dem Immaterialgüterrecht weithin bekannten „Hamburger Brauchs“⁹⁶ erfolgen, um das Gegenüber nicht durch eine bezifferte (ggf. sehr hohe) Vertragsstrafe zu irritieren.⁹⁷

1. Partei B wird das Modell [XY] vertraulich behandeln und nur für den vertraglich vereinbarten Zweck verwenden. Sie wird alle erforderlichen und zumutbaren Maßnahmen treffen, um die Offenlegung

des Modells gegenüber Dritten und/oder die Verwertung des Modells durch Dritte zu verhindern. Zulässig ist die Offenlegung des Modells nur gegenüber solchen Mitarbeitern, Angestellten und externen Beratern der Partei B, die unmittelbar mit der Vertragsdurchführung befasst sind (need to know). Diese sind, wenn sie nicht von Berufs wegen zur Verschwiegenheit verpflichtet sind, schriftlich zur Einhaltung mindestens der Geheimhaltungspflichten nach diesem Vertrag zu verpflichten. Die Offenlegung von Vertraulichen Informationen ist auch zulässig, falls und soweit Partei B aufgrund einer Rechtsvorschrift oder behördlichen Anordnung dazu verpflichtet ist, den Anbieter über die beabsichtigte Offenlegung schriftlich informiert hat und nach dem Gesetz vorgesehene und/oder angemessene Vorkehrungen getroffen hat, um den Umfang der Offenlegung so gering wie möglich zu halten. Im Übrigen ist die Offenlegung gegenüber Dritten nur nach vorheriger schriftlicher Zustimmung des Anbieters zulässig.

2. Absatz 1 gilt nicht, wenn und soweit Partei B nachweist, dass das Modell:
 - a. bereits zum Zeitpunkt der Kenntniserlangung allgemein bekannt war oder zu einem späteren Zeitpunkt und ohne Verletzung der Verpflichtungen aus diesem Vertrag allgemein bekannt wurde,
 - b. der Partei B im Zeitpunkt der Kenntniserlangung bereits ohne Verstoß gegen Geheimhaltungsverpflichtungen bekannt war,
 - c. von Partei B eigenständig und unabhängig, d. h. ohne Nutzung des Modells oder Verweis darauf, entwickelt wurde,
 - d. Partei B durch Dritte zugänglich gemacht wurde, welche das Modell rechtmäßig erlangt haben und zur Offenlegung befugt waren.
3. Partei B wird nach Beendigung dieses Vertrags unverzüglich und auf eigene Kosten das Modell (inklusive aller Kopien) zerstören und dies dem Anbieter bestätigen. Dies gilt nicht, wenn Partei B zur Aufbewahrung des Modells gesetzlich verpflichtet ist; in diesem Fall wird Partei B den Anbieter darüber unverzüglich in Kenntnis setzen und Satz 1 mit Wegfall der gesetzlichen Pflicht erfüllen. Ein Zurückbehaltungsrecht steht Partei B nicht zu.

⁹⁴ LAG Düsseldorf GRUR-RS 2020, 23408 – das Urteil mag aber auch implizit durch die auch unter dem GeschGehG zu beachtenden Besonderheiten des Arbeitsrechts (Treuepflicht des Arbeitnehmers) geprägt sein.

⁹⁵ Rhetorisch gefragt: Wie vertrauenswürdig ist jemand, der es ablehnt, für den Fall des Vertraulichkeitsbruchs eine Pönale zu entrichten?

⁹⁶ Dieser ist zweifelsohne auch AGB-rechtlich zulässig, zumal im geschäftlichen Verkehr, vgl. nur BGH GRUR 2014, 595 – Vertragsstrafenklausel.

⁹⁷ Zum AGB-rechtlich problematischen (s. oben 5.c) Ausschluss der Möglichkeit zum Reverse Engineering (§ 3 I 2 GeschGehG) s. den Klauselvorschlag von Schubert in BeckOF, IT- und Datenrecht, 4. Ed. 2020, 3.3.

4. Die Geheimhaltungspflichten nach diesem Vertrag enden fünf Jahre nach Beendigung dieses Vertrags.
5. Mit jedem einzelnen, schuldhaften Verstoß gegen die in diesem Vertrag enthaltenen Geheimhaltungspflichten verurteilt Partei B eine Vertragsstrafe, deren Höhe vom Anbieter in jedem Einzelfall nach billigem Ermessen festgesetzt wird und die im Streitfall von einem zuständigen Gericht überprüft werden kann. Die Höhe der Vertragsstrafe im Einzelfall wird einen Betrag von EUR [...] nicht übersteigen (in Worten: Euro [...]). Die Vertragsstrafe wird auf etwaige sonstige Schadensersatzansprüche, die dem Anbieter aus diesem Verstoß entstehen, angerechnet. Weitergehende, über die Vertragsstrafe hinausgehende Schadensersatzansprüche vom Anbieter bleiben unberührt.
6. § 5 GeschGehG bleibt durch diese Klausel unberührt.⁹⁸

2. Trainieren mit Trainingsdaten des Vertragspartners

[46] *Vorbemerkung:* Liefert ein Vertragspartner Daten an den Anbieter eines Modells, so ist es naheliegend, dass Letztgenannter mit diesen Daten trainieren möchte, um die Qualität des Modells zu verbessern. Erhält ein Anbieter etwa Dokumente zum Schwärzen, so wäre es für den Anbieter wirtschaftlich vorteilhaft, dass sein eingesetzter Algorithmus die beim Schwärzen gewonnenen Erkenntnisse auch bei der Bearbeitung künftiger Dokumente erneut einsetzen könnte. Die Vertragspartner des Anbieters haben hieran naturgemäß wenig Interesse, was sich in der Praxis aber dann ändern kann, wenn die Nutzung ihrer Daten zu Trainingszwecken als Teil des Entgelts an den Anbieter qualifiziert wird und das Entgelt für die eigentliche Dienstleistung damit sinkt. Trotzdem müssen Geheimhaltungsinteressen natürlich gewahrt werden, was wiederum die Nutzbarkeit der Trainingsdaten im Modell nicht einschränken darf. Stößt die nachfolgende Klausel aus Sicht des Anbieters auf Widerstand, empfiehlt es sich, den Umfang der Daten zu begrenzen, etwa durch eine Pseudonymisierung oder Anonymisierung. Dies ist bei Machine Learning häufig ohnehin geboten, da Daten wie Namen, E-Mail-Adressen oder Telefonnummern auf Grund ihres zufälligen Charakters fast nie Gegenstand von selbstlernenden Algorithmen sind.

[47] Für die Praxis bietet sich folgende Klausel an:

Partei B gestattet dem Anbieter, mit [den Daten] das Modell⁹⁹ des Anbieters weiter zu trainieren, Korrelationen aus [den Daten] herzuleiten und mit dem sodann verbesserten Modell nach freiem Belieben zu verfahren. Partei B ist sich bewusst, dass es technisch äußerst aufwendig, aber nicht völlig unmöglich ist, aus dem verbesserten Modell Rückschlüsse auf einzelne Daten

von Partei B zu ziehen. Insoweit verzichtet Partei B auf alle Rechte am Modell und gegenüber dem Anbieter [und stellt sicher, dass auch andere Inhaber von Rechten an [den Daten] dies tun].

3. Nutzungslizenz

[48] *Vorbemerkung:* Obgleich Modelle typischerweise nicht urheberrechtlich geschützt sind, besteht ein Bedarf, dass Anbieter Dritten Zugriffs- und Nutzungsrechte einräumen. Dies lässt sich durch eine vertraglich ausgestaltete Lizenz grundsätzlich regeln. Um sich nicht dem Vorwurf einer anfänglich und rechtlich unmöglichen Leistung i. S. d. § 275 I BGB auszusetzen mit dem Argument, ein Modell sei nicht urheberrechtlich geschützt und ein Nutzungsrecht daran könne deswegen nicht eingeräumt werden und betreffe daher nur ein Scheinrecht,¹⁰⁰ ist dem Anbieter eine Klarstellung zu empfehlen: Die Lizenz bezieht sich nicht auf vermeintlich urheberrechtlich geschützte Werke, sondern es wird stattdessen eine wirtschaftliche Vorzugsstellung eingeräumt. Rechtsdogmatisch ist diese darin zu sehen, dass "das Interesse des Lizenznehmers regelmäßig nicht so sehr auf die Zusage des Rechtsbestands des Schutzrechts, sondern eher auf die Erlaubnis zur Benutzung des Schutzgegenstands gerichtet ist".¹⁰¹ Dieser Aspekt sollte in der Regelung zum Vertragsgegenstand betont werden.

[49] Wegen der alleine *inter partes* wirkenden Einräumung einer solchen Nutzungsbefugnis empfiehlt sich die Absicherung über eine Geheimhaltungsklausel,¹⁰² um zu verhindern, dass Dritte in den Besitz eines Modells kommen und mangels vertraglicher Bindung an den Lizenzgeber nach Belieben mit dem Modell verfahren können, ohne gegen Recht zu verstoßen.

[50] Dies vorausgeschickt könnte ein Lizenzklausel für einen Vertrag über die Überlassung eines sonstigen Gegenstandes, dem KI-Modell, lauten:¹⁰³

Gegenstand dieses Vertrages ist die Einräumung einer tatsächlichen Nutzungsbefugnis am Modell [XY], die eine wirtschaftliche Vorzugsstellung des Lizenznehmers begründet. Die Nutzungsbefugnis ist nicht unterlizenzierbar, nicht ausschließlich, nicht übertrag- und vermietbar, zeitlich beschränkt [bis 31.12.2020] und räumlich beschränkt auf [das Gebiet der Bundesrepublik Deutschland].

⁹⁸ Vgl. *Apel/Boom GRUR-Prax* 2020, 225.

⁹⁹ Hier bieten sich auch untechnische, aber womöglich besser verständliche Begriffe wie "Algorithmen" oder "Software" an.

¹⁰⁰ Vgl. die Ausführungen bei *BGH NJW* 2012, 3512 (3514) mit allerdings gegenteiligem Ergebnis.

¹⁰¹ *BGH NJW* 2012, 3512 (3514).

¹⁰² Angelehnt an Kaulartz/Braegelmann/Schicker, *Rechtshandbuch Artificial Intelligence und Machine Learning*, Kap. 7.2 Rn.6.

¹⁰³ Angelehnt an Kaulartz/Braegelmann/Schicker, *Rechtshandbuch Artificial Intelligence und Machine Learning*, Kap. 7.2 Rn. 4.

VII. Zusammenfassung und Schluss

[51] Durch Künstliche Intelligenz wird bis 2030 eine Steigerung der Wirtschaftsleistung um 13 Milliarden US-Dollar vorausgesagt.¹⁰⁴ Unter Berücksichtigung der Relevanz von Machine Learning bedeutet dies eine hohe Relevanz für den rechtlichen Schutz von Machine Learning-Modellen. Der Beitrag hat gezeigt, dass dieser *de lege lata* derzeit verlässlich nur darüber erreicht werden kann, dass solche Modelle als Geschäftsgeheimnisse im Sinne des GeschGehG geschützt werden; nur ausnahmsweise können Unternehmen sich auf einen datenbankrechtlichen Schutz berufen. Die Folge sind steigende Anforderungen an technische, organisatorische und rechtliche¹⁰⁵ Maßnahmen zum Schutz der Modelle. Werden diese nicht umgesetzt,

kann es in der Praxis schwierig werden, das unzulässige Verwenden von Modellen straf- oder zivilrechtlich zu verfolgen.

[52] Unternehmen ist dringend zu raten, unter dem Stichwort „AI Compliance“ interne Prozesse zu etablieren und Maßnahmen zu dokumentieren, die nicht nur für eine vertrauenswürdige KI¹⁰⁶ sorgen, sondern auch ihre Modelle technisch und rechtlich schützen. Der Beitrag hat hierzu einige Vorschläge unterbreitet.

¹⁰⁴ *McKinsey Global Institute*, Notes from the AI Frontier – Tackling Europe’s Gap in Digital and AI, 2019, 29.

¹⁰⁵ Namentlich: Vertragliche.

¹⁰⁶ Unabhängige Hochrangige Expertengruppe für Künstliche Intelligenz, 2018, Ethik-Leitlinien für vertrauenswürdige KI; EU Kommission, Weissbuch zur Künstlichen Intelligenz – ein europäisches Konzept für Exzellenz und Vertrauen, 2020, COM(2020) 65.

Prof. Dr. Florian Möslein*

Die normative Kraft des Ethischen

Ein Fallbeispiel zur Effektivität von Leitlinien für Künstliche Intelligenz

Ethische Leitlinien für den Umgang mit künstlicher Intelligenz haben derzeit Konjunktur. Sie entstehen auf ganz unterschiedlichen Regelungsebenen und auf Initiative ganz unterschiedlicher Regelgeber. Prominente Beispiele sind die OECD-Empfehlungen zu künstlicher Intelligenz und die Ethik-Leitlinien für eine vertrauenswürdige KI der von der Europäischen Kommission eingesetzten Hochrangigen Expertengruppe für Künstliche Intelligenz; zusätzlich gibt es mehr und mehr Leitlinien einzelner Unternehmen und Verbände. Aber welche normative Kraft haben solche ethischen Leitlinien? Welche rechtliche Wirkung entfalten sie; welche Folgen zieht ihre Nichteinhaltung gegebenenfalls nach sich? Diesen Fragen geht der nachfolgende Beitrag anhand eines unternehmensrechtlichen Fallbeispiels auf den Grund.

I. Einführung

[1] Der Titel dieses Beitrags nimmt Bezug auf die berühmte Formel von der „normativen Kraft des Faktischen“. Sie geht zurück auf *Georg Jellineks* Allgemeine Staatslehre aus dem Jahr 1900, einem Klassiker der

Rechts- und Sozialwissenschaft.¹ *Jellinek* begründet die Geltung verbindlicher Normen mit der Eigenschaft des Menschen, das „ihn stets Umgebende, das von ihm fortwährend Wahrgenommene, das ununterbrochen von ihm Geübte nicht nur als Tatsache, sondern auch als Beurteilungsnorm“ anzusehen, „an der er Abweichendes prüft, mit der er Fremdes richtet“.² Fortdauernde Übung erzeugt demnach „die Vorstellung des Norm-

* Der Autor (LL. M. (London)) ist Inhaber der Professur für Bürgerliches Recht, Deutsches und Europäisches Wirtschaftsrecht an der Philipps-Universität Marburg. Er ist einer der beiden Gründungsdirektoren des dortigen Instituts für das Recht der Digitalisierung (IRDi) sowie Direktor des Instituts für Handels-, Wirtschafts- und Arbeitsrecht; er ist zudem stellvertretender Leiter des hessischen Kompetenzzentrums für verantwortungsbewusste Digitalisierung sowie einer der geschäftsführenden Herausgeber der RD*i*. Der Beitrag beruht auf einem Vortrag des Autors am 23. Juni 2020 an der Universität des Saarlandes. Sämtliche Internetquellen wurden am 27.10.2020 zuletzt abgerufen.

¹ G. *Jellinek*, Allgemeine Staatslehre, 1900, bes. S. 337 ff.; dazu näher *Anter* (Hrsg.), Die normative Kraft des Faktischen, 2004; zur bleibenden Bedeutung ferner: *Kersten*, Georg Jellinek und die klassische Staatslehre, 2000, S. 1-11, 178-186, 303-307 und 444-451; *Paulson/Schulte/Möllers*, Georg Jellinek – Beiträge zu Leben und Werk, 2000, S. 155-171.

² G. *Jellinek*, Allgemeine Staatslehre, S. 337.

mäßigen dieser Übung, und es erscheint damit die Norm selbst als autoritäres Gebot des Gemeinwesens, also als Rechtsnorm“.³ Ebendieser normativen Kraft des Faktischen räumt *Jellinek* für die Entwicklung von Recht und Sittlichkeit, aber auch für die Geltung und Effektivität von Normen höchste Bedeutung ein.

[2] 120 Jahre später sind Normentwicklungsprozesse besonders mit Bezug auf digitale Technologien und vor allem auf dem Gebiet der Künstlichen Intelligenz (KI) zu verzeichnen.⁴ Die technische Entwicklung verläuft so rasant, ja buchstäblich disruptiv, dass es an einer fort-dauernden Übung im Umgang mit KI vorerst allerdings noch fehlt. Als Ersatz werden so genannte ethische Leitlinien für den Umgang mit künstlicher Intelligenz formuliert, und zwar auf ganz unterschiedlichen Regelungsebenen und von ganz unterschiedlichen Regelgebern. Prominente Beispiele sind die OECD-Empfehlungen zu künstlicher Intelligenz vom 22. Mai 2019,⁵ die europäischen Ethik-Leitlinien, die eine von der EU-Kommission eingesetzte hochrangige Expertengruppe für künstliche Intelligenz am 8. April 2019 in vorerst finalisierter Fassung veröffentlicht hatte⁶ und deren zentrale Forderungen die Kommission zuletzt in ihrem KI-Weißbuch ausdrücklich unterstützt,⁷ oder auch die Leitlinien des Bundesverbands Digitale Wirtschaft und einzelner Unternehmen wie Daimler, Deutsche Telekom und Google.⁸ Die Regelungsinhalte erstrecken sich insbesondere auf Grundsätze der Technikbeherrschbarkeit und -beherrschung, auf Offenlegungs- und Rechenschaftspflichten sowie auf Wahrung bestimmter Individualrechte und Gemeinwohlbelange. Im Detail finden sich freilich Unterschiede zwischen den einzelnen Regelwerken. Weil die vielfältigen Normentwicklungsprozesse und Norminhalte ungemein schwer zu überblicken sind, gibt es Versuche einer kartographischen Erfassung, etwa seitens des *Berkman Klein Center for Internet and Society* der Universität Harvard.⁹

[3] Vor allem wirft diese Normenvielfalt Fragen der Effektivität auf, wie sie einst schon *Georg Jellinek* beschäftigt haben. Bereits über die Verwendung des Begriffs der Ethik mag man streiten, weil sich ethische Normen formal gerade dadurch auszeichnen, dass sie „nicht durch ein grundsätzlich dazu befugtes Rechtssetzungsorgan gesetzt werden“.¹⁰ Die wichtigsten Leitlinien wurden jedoch von oder unter Beteiligung von supranationalen bzw. staatlichen Institutionen entwickelt. Die Unterscheidung zwischen hoheitlich gesetzten und faktisch entstanden Normen verwischt freilich gerade bei *Jellinek*, der zwischen Normativität und Faktizität zu vermitteln versucht.¹¹ Völlig unklar ist dagegen eine Frage, die *Jellinek* wohl besonders interessiert hätte, nämlich welche normative Kraft jene ethischen Leitlinien haben können. Wie kontrovers sich ihre Geltungskraft (und umgekehrt der verbleibende gesetzliche Regulierungsbedarf) einschätzen lässt, zeigt die Gegen-

überstellung zweier zentraler rechtspolitischer Stellungnahmen: Während die einflussreiche Initiative D21 in ihren Leitlinien zum ethischen Umgang mit Algorithmen-Monitoring neue gesetzliche Regelungen für KI nachdrücklich ablehnt und die Formulierung ethischer Grundsätze für ausreichend hält,¹² vertritt die Datenethikkommission in ihrem Abschlussgutachten genau den gegenteiligen Standpunkt, dass nämlich „ethische Grundsätze und Prinzipien rechtliche Regulierung nicht entbehrlich machen können“.¹³ Welche dieser beiden Positionen zutrifft, lässt sich nicht pauschal beantworten, sondern hängt auch vom Einzelfall ab, etwa von den Funktionalitäten und Einsatzbereichen der jeweiligen technologischen Anwendung, von den jeweils betroffenen Rechtsgütern und auch vom Schutzbedürfnis der beteiligten Individuen. Unabhängig von diesen Einzelumständen ist für den gesetzlichen Regelungsbedarf dennoch entscheidend, welche normative Kraft jenen ethischen Leitlinien zukommt.

[4] Diese normative Kraft hängt zum einen vom Befolungsgrad ab, also von der empirischen Frage, in welchem Umfang KI-Systeme programmiert werden, die mit bestimmten ethischen Leitlinien im Einklang stehen. „Die fortdauernde Übung erzeugt die Vorstellung des Normmäßigen dieser Übung, und es erscheint damit die Norm selbst als autoritäres Gebot des Gemeinwesens, also als Rechtsnorm“, so schrieb bereits *Jellinek*.¹⁴ Da allerdings die Technologie der Künstlichen Intelligenz vergleichsweise jung ist und auch die ethischen Leitlinien erst seit 2019 entstanden sind, ist die Zeit noch nicht reif, um eine fortdauernde Übung der (Nicht-)Einhaltung die-

³ S. nochmals *G. Jellinek*, Allgemeine Staatslehre, S. 339.

⁴ Zu diesen Entwicklungen näher: *Linardatos/Möslein*, Rechtshandbuch Robo Advice, 2020, S. 58; *ders./M. Horn*, Emerging Rules on Artificial Intelligence, in: *Durovic/ Di Matteo/ Ortolani* u. a. (Hrsg.), *Lawyering in the Digital Age*, in Vorb. f. 2020.

⁵ OECD, Recommendation of the Council on Artificial Intelligence, abrufbar unter: <https://beck-link.de/rv25v>.

⁶ Abrufbar unter: <https://beck-link.de/e6d35>. Grundlage für die Einsetzung dieser Gruppe bildete die Mitteilung der *Europäischen Kommission*, Künstliche Intelligenz für Europa, COM(2018) 237 final, 20.

⁷ *Europäische Kommission*, Weißbuch „Zur Künstlichen Intelligenz – ein europäisches Konzept für Exzellenz und Vertrauen“, COM (2020) 65 final; vgl. außerdem *diess.*, Mitteilung „Schaffung von Vertrauen in eine auf den Menschen ausgerichtete künstliche Intelligenz“, COM (2019), 168 final.

⁸ Die Leitlinien des Bundesverbands sind abrufbar unter <https://beck-link.de/54h3f>; vgl. ferner Daimler, abrufbar unter: <https://beck-link.de/z6ksv>; Telekom, abrufbar unter: <https://beck-link.de/pkte5>; Google, abrufbar unter: <https://beck-link.de/ne6tm>.

⁹ Dazu ausführlich und mit Visualisierung unter <https://ai-hr.cyber.harvard.edu/>.

¹⁰ *Vöney/Beylage-Haarmann/Höfelmeier/Hübler/Vöney*, Ethik und Recht – Die Ethisierung des Rechts, 2013, S. 129, 132.

¹¹ *Jellinek*, Allgemeine Staatslehre, S. 342; s. dazu etwa *Lepsius*, Besitz und Sachherrschaft im öffentlichen Recht, 2002, S. 178; *Brugger/Gröschner/Lembcke/v. Klink/Lembcke*, Faktizität und Normativität. *Georg Jellineks* freiheitliche Verfassungslehre, 2016, S. 63.

¹² *Initiative D21*, #Algomon: 9 Leitlinien zum Ethischen Umgang mit Algorithmen-Monitoring, 2019, abrufbar unter: <https://beck-link.de/tbx4d>, unter Nr. 5.

¹³ *Datenethikkommission*, Gutachten, 2019, abrufbar unter: <https://beck-link.de/p3zh2>, dort S. 13.

¹⁴ *Jellinek*, Allgemeine Staatslehre, S. 339.

ser Leitlinien glaubwürdig konstatieren zu können. Auf der anderen Seite hängt die Effektivität von Normen entscheidend von deren Sanktionierung ab, also von der Frage, ob derjenige, der von der Leitlinie abweicht, allenfalls Reputationsverluste befürchten muss, oder ob ihm weitergehende, auch rechtliche Sanktionen drohen. Dass *ethische* Leitlinien in Frage stehen, schließt solche Sanktionen keineswegs kategorisch aus, auch wenn die Normgeber selbst schematisch zwischen ethischer und rechtskonformer KI zu unterscheiden versuchen. Beispielsweise schreibt die europäische Expertengruppe, ihre Leitlinien beschäftigten sich nicht explizit mit rechtmäßiger KI, sondern sie sollten vielmehr eine Hilfestellung für die Förderung und Sicherung ethischer und robuster KI bieten.¹⁵ Bereits § 138 I BGB zeigt jedoch, dass Rechts- und Sittenordnung nicht zusammenhanglos nebeneinanderstehen, sondern dass soziale, moralische und auch ethische Wertungen – jedenfalls das „Anstandsgefühl aller billig und gerecht Denkenden“ –¹⁶ durchaus auch rechtliche Wirkung entfalten.¹⁷ Ob auch die genannten KI-Leitlinien solche Wirkung entfalten, soll im Folgenden ausgemessen werden, und zwar an einem Fallbeispiel mit gesellschaftsrechtlichem Bezug. Die rechtstheoretische Schwierigkeit dieser Vermessung besteht in der Besonderheit, dass die ethischen Normen nicht durch faktische Übung „von unten“ gewachsen sind, sondern von bzw. unter Beteiligung von staatlichen Akteuren und supranationalen Organisationen erdacht und verschriftlicht worden sind – aber mangels Gesetzesqualität dennoch zum sog. *ius non scriptum* zählen.¹⁸

II. Fallbeispiel „Vital“

[5] Gewisse Berühmtheit hat der KI-Algorithmus Vital erlangt, an den das Fallbeispiel anknüpft: Die Venture-Capital-Gesellschaft Deep Knowledge Ventures hatte diesen Algorithmus im Jahr 2014 in ihren Vorstand berufen.¹⁹ Jedenfalls berichteten die Medien, Vital habe volles Stimmrecht eingeräumt bekommen und könne über Unternehmensinvestitionen mitentscheiden.²⁰ Grund war Vitals' Fähigkeit „to automate due diligence and use historical data-sets to uncover trends that are not immediately obvious to humans surveying top-line data“.²¹ Er hat also bei der Auswahl und Finanzierung der einzelnen Start-Ups mitgewirkt, in die das Unternehmen investierte.²² Entgegen den Medienberichten hatte Vital nach dem anwendbaren Gesellschaftsrecht allerdings weder echtes Stimmrecht noch die rechtliche Stellung eines Vorstandsmitglieds. In Wahrheit hatten die menschlichen Vorstandsmitglieder lediglich beschlossen, ihn als eine Art Beobachter in ihre Entscheidungen einzubeziehen.²³

[6] Weil Vital gleichwohl als „the world's first artificial intelligence company director“ gilt,²⁴ kann sein Beispiel dazu dienen, hypothetisch weiterzudenken. Nehmen wir an, Vital's Investitionsentscheidungen erwiesen sich als wirtschaftlich erfolgreich, so dass die menschlichen Vor-

standsmitglieder ihnen immer mehr vertrauen. Nach einiger Zeit werden allerdings Befürchtungen laut, Vital bevorzuge Start-Ups mit weißen, männlichen Gründern, während dunkelhäutige oder weibliche Gründer systematisch benachteiligt würden. Außerdem stellt sich heraus, dass Vital den Vorstand davon hatte überzeugen können, in ein Start-up zu investieren, das die Behandlung altersbedingter Krankheiten erforschte, dabei allerdings äußerst fragwürdige Tierversuche durchführte. Der Aufsichtsrat der Deep Knowledge Ventures Aktiengesellschaft verlangt vom Vorstand daraufhin umfassende Auskunft; er möchte insbesondere über Funktionsweise und Entscheidungsfindung von Vital informiert werden. Zudem überlegt er, ob die Einbindung künstlicher Intelligenz in Vorstandsentscheidungen überhaupt zulässig ist, und ob er den Vorstand für die getroffenen Entscheidungen in die Pflicht nehmen kann.

III. Aktienrechtlicher Rahmen

1. Zulässigkeit von Delegation

[7] Zunächst wirft das Fallbeispiel die Frage auf, ob der Vorstand die fraglichen Entscheidungen an Vital delegieren durfte.²⁵ Allgemein gilt Delegation im Aktienrecht als „Gebot praktischer Vernunft“,²⁶ weil Unternehmensleitung ohne Delegation kaum zu bewältigen wäre. Die Delegationsbefugnis findet allerdings Grenzen, die sich aus dem aktienrechtlichen Grundsatz umfassender Leitungsverantwortung ableiten lassen. So

¹⁵ Leitlinien (Fn. 6), S. 8 (Rn. 24).

¹⁶ St. Rspr seit RGZ 48, 114 (124); neuerdings etwa BGH NJW 2004, 2668 (2670).

¹⁷ Vgl. etwa Eckert, AcP 199 (1999), 337 (345): „bindende Verknüpfung des Rechts mit den Geboten der Sittlichkeit, [...] der bürgerlichen Moral“; sowie bereits Coing NJW 1947/48, 213 (Fallgruppe der „Verletzung ethischer Güter“).

¹⁸ Entscheidend ist hierfür nämlich nicht die äußere Form, sondern ob „ein Rechtssatz durch Ausspruch der gesetzgebenden Gewalt Autorität“ bekommt, so bereits Savigny, Pandektenvorlesung, 1824/1825, S. 11; vgl. außerdem Meder, *Ius non scriptum*, 2. Aufl. 2009, S. 9 f.

¹⁹ S. beispielsweise Möslein ZIP 2018, 204 (206 f.); Barfield/Pagallo/Möslein, *Research Handbook on the Law of Artificial Intelligence*, 2018, 649 (649 f.); Sattler BB 2018, 2243 (2248); Strohn ZHR 182 (2018), 371; Weber/Kiefner/Jobst NZG 2018, 1131 (1136).

²⁰ Wile, „A Venture Capital Firm Just Named an Algorithm to its Board of Directors“, *Business Insider*, 13.5.2014, abrufbar unter: <https://beck-link.de/xht58>.

²¹ Zolfagharifard, „Would you take orders from a Robot? An artificial intelligence becomes the world's first company director“, *Daily Mail*, 19.5.2014, abrufbar unter: <https://beck-link.de/b85zs>.

²² Zu Einzelheiten vgl. die Pressemitteilung der *Biogerontology Research Foundation*, „Deep Knowledge Ventures announces new investment fund for life sciences and aging research“, *EurekaAlert!*, 16.12.2015, abrufbar unter: <https://beck-link.de/3se53>.

²³ Vgl. D. Kaminsky, Gründungspartner von Deep Knowledge Ventures, zitiert nach Burrige, „Artificial intelligence gets a seat in the boardroom“, *Nikkei Asian Review*, 10.5.2017, abrufbar unter: <https://beck-link.de/c7727>: „as a member of [the] board with observer status“.

²⁴ S. nochmals Zolfagharifard (Fn. 21).

²⁵ Vgl., auch zum Folgenden: Ebers/Heinze/Krügel/Steinrötter/Möslein, *Künstliche Intelligenz und Robotik*, 2020, § 13, Rdn. 24 ff.; Braegelmann/Kaulartz/Möslein, *Rechtshandbuch Artificial Intelligence und Machine Learning*, 2020, S. 509 (511 f.).

²⁶ In diesem Sinne Fleischer ZIP 2003, 1 (8); Geßler FS Hefermehl, 1976, 263 (273); Schwark ZHR 142 (1978), 203 (217).

gelten Aufgaben, die das Gesetz ausdrücklich dem Vorstand zuweist oder die als originäre Leitungsaufgaben zählen, der Delegation als nicht zugänglich. Vorbereitungs- und Ausführungsmaßnahmen dagegen dürfen nachgeordneten Unternehmensebenen überlassen werden, sofern der Vorstand „nur am Schluss wohlwogen und in eigener Verantwortung entscheidet“.²⁷ Die genaueren Anforderungen formuliert der BGH großzügig. So hielt er es in einem Urteil zu Personengesellschaften für unbedenklich, wenn ein Dritter, der in weitem Umfang mit Geschäftsführungsaufgaben betraut wird, bei Erfüllung dieser Aufgaben weder Einzelweisungen unterliegt noch jederzeit abberufen werden kann.²⁸ Es sei ausreichend, dass die Führung dieser Geschäfte durch Richtlinien bestimmt und mit Hilfe umfassender Informations- und Kontrollrechte überwacht werden könne.²⁹ Nach dieser Rechtsprechung ist eigenes Ermessen des Delegaten unschädlich, solange dieses Ermessen innerhalb vordefinierter Leitlinien besteht, deren Einhaltung systematisch überwacht wird.³⁰ Die gleichen Grundsätze sollen für Kapitalgesellschaften gelten. Entsprechend hat die Rechtsprechung die Übertragung der gesamten Datenverarbeitung auf eine andere Gesellschaft für zulässig gehalten, sofern nur sichergestellt ist, dass die Qualität der Datenverarbeitung und der Informationsfluss in gleicher Weise gewährleistet sind wie bei Vorhandensein einer eigenen EDV.³¹

2. Delegation an Technologien

[8] Überträgt man diese Grundsätze auf den Einsatz von KI, so ist gleichermaßen zu fordern, dass die menschlichen Geschäftsleiter „Herren des Verfahrens“ bleiben und die Letztentscheidungskompetenz behalten.³² Eine rechtlich bindende Selbstverpflichtung – etwa in der Art, dass Entscheidungen der KI zwingend Berücksichtigung finden – wäre mit der Leitungsverantwortung des Vorstands nicht zu vereinbaren. Im Übrigen ist die Grenzlinie zwischen lediglich beratendem Technikeinsatz, der „immer zulässig und rechtlich unproblematisch“ sein soll, und Delegation „mit Bindungswirkung“ jedoch schwer zu ziehen.³³ Computertechnologien vermögen das Beurteilungsverhalten von Menschen zu beeinflussen, auch wenn sie keine Entscheidungen erzwingen.³⁴ Die Intensität der rechtlichen Anforderungen hängt gleichwohl von der Frage ab, wie viel Entscheidungsmacht die menschlichen Geschäftsleiter rechtlich oder auch faktisch zurückbehalten.³⁵ Eine wichtige Besonderheit besteht darin, dass sich künstliche Intelligenz durch rechtliche Gestaltung weniger gut einfangen lässt als bei menschlichen Delegaten. Richtlinien oder Abberufungsklauseln sind bei der Entscheidungsdelegation an VITAL nicht vorstellbar. Diese Form der Delegation ist lediglich technisch steuerbar; der technische Code gibt den Rahmen vor, innerhalb dessen VITAL agiert. Es hängt daher von Programmierung, Lernalgorithmen und Datenmaterial, nicht jedoch

von Rechtsregeln, ab, nach welchen Maßstäben VITAL entscheidet. Wer als Vorstand Entscheidungen an KI delegieren will, muss deshalb ein gewisses Maß an Technikbeherrschung besitzen, um die Eigenlogik der Algorithmenentscheidung begreifen und dadurch seine eigene Letztentscheidungskompetenz bewahren zu können.³⁶

3. Lernfähigkeit der KI

[9] Aktienrechtliche Besonderheiten könnten sich aus dem selbstlernenden Charakter künstlicher Intelligenz ergeben:³⁷ Die bedenklichen Entscheidungsmuster hat VITAL in unserem Fallbeispiel erst im Lauf der Zeit entwickelt. Auf Grund der Eigendynamik, die selbstlernende Systeme entwickeln, um Fehler zu erkennen und selbsttätig abzustellen, sind deren Ergebnisse weder programmier- noch vorhersehbar. Solche Systeme sind bekanntlich eine Art „Black Box“, die KI zwangsläufig schwer beherrsch- und damit auch erklärbar macht.³⁸ Zugleich ermöglicht erst diese Fähigkeit des Selbstlernens die stetige Fortentwicklung und Verbesserung der technologiebasierten Entscheidungsempfehlungen. Vorstände hinsichtlich des Einsatzes solcher Technologien zu einem Totalverzicht zu verpflichten, erschiene daher trotz der potenziellen Risiken widersinnig.³⁹ Außer Frage steht der Einsatz von KI jedenfalls, wenn die Satzung ihn ausdrücklich vorsieht und er daher zweifelsfrei dem Willen der Anteilseigner entspricht.⁴⁰ Besteht der statutarische Unternehmensgegenstand von Deep Knowledge Ventures beispielsweise in der KI-basierten Entwicklung von Investmentstrategien, die überhaupt nur mittels

²⁷ So *Fleischer* ZIP 2003, 1 (6); Spindler/Stilz/*Fleischer*, AktG, 4. Aufl. 2019, § 93 Rn. 99; MüKoGmbHG/*Fleischer*, 3. Aufl. 2019, § 43 Rn. 123; vgl. auch *Henze* BB 2000, 2009 (2010).

²⁸ *BGH* NJW 1982, 1817; vgl. außerdem bereits *BGHZ* 36, 293 = NJW 1962, 738.

²⁹ Vgl. nochmals *BGH* NJW 1982, 1817 (1818).

³⁰ Näher etwa *Otte-Gräbener/Deilmann* NZG 2016, 1361 (1362).

³¹ *LG Darmstadt* ZIP 1986, 1389 (1391 f.); vgl. auch *Henze* BB 2000, 209 (209 f.).

³² Vgl., auch zum Folgenden: Ebers/Heinze/Krügel/Steinrötter/*Möslein*, Künstliche Intelligenz und Robotik, 2020, § 13, Rdn. 27 ff.; Braegelmann/Kaulartz/*Möslein*, Rechtshandbuch Artificial Intelligence und Machine Learning, 509 (512 f.).

³³ So jedoch *Zetsche* AG 2019, 1 (7).

³⁴ Zum Phänomen der sog. „Persuasive Technologies“ näher *Fogg*, *Persuasive Technology: Using Computers to Change What We Think and Do*, 2003; vgl. auch die Forschungsagenda des *Persuasive Technology Lab* an der Universität Stanford, <http://captology.stanford.edu/>.

³⁵ Zu den Abstufungen vgl. *Weber/Kiefner/Jobst* NZG 2018, 1131 (1134).

³⁶ Allgemeiner zu Leitungspflichten in Zeiten digitaler Veränderung M. Hilb/*ders.*, *Governance of Digitalization*, 2017, 11 (20); M. Hilb/*R. Müller*, *Governance of Digitalization*, 2017, S. 43; *Featherstone*, „Governance in the new machine age“, Australian Institute of Company Directors, 24.3.2017, abrufbar unter: <https://beck-link.de/ezhy3>.

³⁷ Näher zu dieser Besonderheit Ebers/Heinze/Krügel/Steinrötter/*Möslein*, Künstliche Intelligenz und Robotik, 2020, § 13, Rdn. 29; Braegelmann/Kaulartz/*Möslein*, Rechtshandbuch Artificial Intelligence und Machine Learning, 509 (513).

³⁸ *Strohn* ZHR 182 (2018), 374.

³⁹ S. auch Braegelmann/Kaulartz/*Möslein*, Rechtshandbuch Artificial Intelligence und Machine Learning, 509 (513).

⁴⁰ Näher Ebers/Heinze/Krügel/Steinrötter/*Möslein*, Künstliche Intelligenz und Robotik, § 13, Rdn. 30

Entscheidungsdelegation an Algorithmen erreichbar ist, so steht die Zulässigkeit des KI-Einsatzes von vorneherein außer Frage.

IV. Vorstandspflichten bei KI-Entscheidungen

1. Normative Grundlage

[10] Soweit Delegation nach diesen Grundsätzen zulässig ist, stellt sich die Frage, wer für delegierte Entscheidungen haftet, sofern sich die fragliche, an künstliche Intelligenz delegierte Entscheidung im Nachhinein als fehlerhaft herausstellt – sei es, weil sie sich für die Gesellschaft als wirtschaftlich nachteilig erweist oder aber, weil sie inhaltlich fragwürdig erscheint.⁴¹ Wenn Vital nach Hautfarbe und Geschlecht diskriminiert oder zu Gunsten eines Unternehmens entscheidet, das fragwürdige Tierversuche durchführt, liegt der Fokus auf der inhaltlichen Fragwürdigkeit, sind aber angesichts der Reputationseffekte auch wirtschaftlich nachteilige Konsequenzen denkbar. Der Aufsichtsrat (möglicherweise auch das Aktionariat) steht nach solchen Entscheidungen vor der Frage, ob der Vorstand – oder der Algorithmus selbst? – für entstandene Verluste einstehen muss, und allgemeiner, ob Pflichten im Rechtssinne verletzt worden sind. Da der Sachverhalt zunächst weiterer Aufklärung bedarf, lautet die Vorfrage, ob und in welchem Umfang der Vorstand über die betreffenden Vorgänge Rechenschaft schuldet.

[11] Als Pflichtadressat kommt der Algorithmus selbst nicht in Frage, weil (bzw. soweit) künstliche Intelligenz keine Rechtsfähigkeit besitzt.⁴² Denkbar scheint jedoch die Zurechnung des Fehlverhaltens des Algorithmus an den Vorstand, der diese Entscheidung delegiert hat. Eine analoge Anwendung von § 278 BGB auf das Versagen von Maschinen wird zwar teils vertreten.⁴³ Sie ist aber mangels Vergleichbarkeit der Interessenlage mit der hM abzulehnen, insbesondere weil KI nicht schuldhaft handeln kann.⁴⁴ Weil Delegaten nicht als Erfüllungsgehilfen des Vorstands tätig werden, sondern ausschließlich im Pflichtenkreis der Aktiengesellschaft handeln, hilft diese Analogie in aktienrechtlichem Zusammenhang ohnehin nicht weiter.⁴⁵ Eine Inanspruchnahme nach § 831 BGB scheidet gleichermaßen aus, weil Geschäftsherr nicht der Vorstand, sondern die Gesellschaft ist.⁴⁶ Entsprechend ist alleine eine Haftung des Vorstands für Eigenverschulden denkbar. Die Pflichtverletzung kann u. a. darin gründen, dass Auswahl, Einweisung oder Überwachung der Delegaten unsorgfältig waren.⁴⁷ Die Überwachungssorgfalt erfordert, dass der Vorstand für laufende Kontrolle sorgt und sicherstellt, dass die übertragenen Aufgaben ordnungsgemäß erfüllt werden.⁴⁸ Aus diesen aktienrechtlichen Grundsätzen lässt sich eine Pflicht zur angemessenen Beherrschung technikimmanenter Risiken ableiten, etwa in Form einer Abschalt-einrichtung. Diese Pflicht lässt sich auch auf den Rechts-

gedanken von § 91 II AktG stützen, der (allerdings im bilanzrechtlichen Zusammenhang) vom Vorstand geeignete Maßnahmen verlangt, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden.⁴⁹ Die Auskunftspflicht gegenüber dem Aufsichtsrat lässt sich auf die allgemeine Regelung des § 90 I 1 AktG stützen, der insbesondere in Nr. 4 Auskunft auch über einzelne Geschäfte fordert, die für Rentabilität oder Liquidität der Gesellschaft von erheblicher Bedeutung sind.⁵⁰

2. Entfaltung

[12] Reichweite und Intensität dieser aktienrechtlichen Überwachungs- und Auskunftspflichten sind für KI-gestützte Entscheidungen noch völlig ungeklärt; sie sind auch allgemein unscharf. Die Rechtsprechung verweist teils lapidar auf „Umstände des Einzelfalls“,⁵¹ was zu Recht als „Leerformel“ kritisiert wird.⁵² Auch die gesetzliche Vorgabe des § 91 II AktG liefert nur einen vagen Anhaltspunkt, begründet aber immerhin eine Pflicht, „technikimmanenten Risiken angemessen zu begegnen“.⁵³ Was der Vorstand von Deep Knowledge Ventures beim KI-Einsatz von Vital konkret hätte tun müssen, um diskriminierende oder gefährdende Investitionsentscheidungen zu verhindern, lässt sich auf dieser rechtlichen Grundlage nicht beantworten, solange Erfahrungssätze zu „angemessenem“ Verhalten im Umgang mit KI fehlen. Eine präzisere Konturierung des Pflichtenprogramms erfordert die Entfaltung spezifischer Einzelpflichten, die bei der Delegation unternehmerischer Entscheidungsaufgaben an Algorithmen zu befolgen sind. Da künstliche Intelligenz ein neues technisches Phänomen darstellt, sind solche Einzelpflichten

⁴¹ Dazu ausführlich Ebers/Heinze/Krügel/Steinrötter/Möslein, Künstliche Intelligenz und Robotik, § 13, Rdn. 35 ff.; Braegelmann/Kaulartz/Möslein, Rechtshandbuch Artificial Intelligence und Machine Learning, 509 (515 ff.).

⁴² Vgl. dazu nur Riehm, Nein zur ePerson! Gegen die Anerkennung einer digitalen Rechtspersönlichkeit, in diesem Heft S. 42.

⁴³ Ausführlich Wolf JuS 1989, 899; vgl. ferner Spiro, Die Haftung für Erfüllungsgehilfen, 1984, S. 211; Schirmer JZ 2016, 660 (664); Günther/Böghmüller BB 2017, 53 (55).

⁴⁴ Lieser JZ 1971, 759 (761); MüKoBGB/Grundmann, 8. Aufl 2019, § 278 Rn. 46; vgl. auch BGH BGHZ 54, 332 = NJW 1971, 32 (zu § 839); BGH BGHZ 99, 249 (254 f.) = NJW 1987, 1945 (für Rechtswidrigkeitshaftung unter Landesrecht).

⁴⁵ Fleck GmbHHR 1974, 224 (225); MüKoGmbHG/Fleischer § 43 Rn. 126; Schulze NJW 2014, 3484 (3486).

⁴⁶ Vgl. BGH BGHZ 125, 366 (375) = NJW 1994, 1801; MüKoGmbHG/Fleischer § 43 Rn. 126; Schulze NJW 2014, 3484 (3486).

⁴⁷ Fleischer/ders., Handbuch des Vorstandsrechts, 2006, § 8 Rn. 28; MüKoGmbHG/Fleischer § 43 Rn. 130; GroßkommAktG/Hopt, 5. Aufl. 2015, § 93 Rn. 55; MüKoAktG/Spindler, 5. Aufl. 2019, § 93 Rn. 98.

⁴⁸ Dreher FS Hopt, 2010, S. 517 (536 f.); Spindler/Stilz/Fleischer AktG § 93 Rn. 104.

⁴⁹ Ähnlich Zetzsche AG 2019, 1 (7 f.).

⁵⁰ Einschränkung jedoch Strohn ZHR 182 (2018), 374.

⁵¹ Vgl. etwa BGH NStZ 1986, 34 – Brückenbau Hopener Mühlenbach.

⁵² So Druey FS Koppensteiner, 2001, S. 3 (8); ebenfalls kritisch Spindler/Stilz/Fleischer AktG § 93 Rn. 104.

⁵³ Zetzsche AG 2019, 1 (7 f.).

vorerst weder positiv-rechtlich normiert noch von der Rechtsprechung entwickelt worden.

[13] Angesichts dieses Regelungsdefizits lässt sich auf zwei denkbare Rechts- bzw. Rechtserkenntnisquellen zurückgreifen: Einerseits ist eine Analogie zu Gesetzesregeln zu erwägen, die algorithmische Entscheidungen in anderem Zusammenhang betreffen.⁵⁴ In Frage kommt vor allem eine Vorschrift des Wertpapierhandelsrechts, die den algorithmischen Handel mit Finanzinstrumenten regelt: § 80 II WpHG sieht eine Reihe von Einzelpflichten vor, die Wertpapierdienstleister erfüllen müssen, die solchen Handel betreiben. Weil hier wie dort Entscheidungen von Algorithmen in Frage stehen, und weil § 80 II WpHG die Verantwortlichkeit für solche Entscheidungen statuiert, ähnelt sich die Interessenlage zumindest im Grundsatz.⁵⁵ Auf der anderen Seite ist ein Rückgriff auf außerrechtliche Verhaltensregeln zu erwägen, namentlich auf die genannte Empfehlung der OECD sowie auf die EU-Leitlinien für eine vertrauenswürdige KI.⁵⁶ Aus diesen beiden Rechtserkenntnisquellen, jenen bestehenden Gesetzesregeln sowie diesen Leitlinien, lassen sich eine Reihe gemeinsamer Grundsätze ableiten, die zur Entfaltung und Konkretisierung unternehmerischer Pflichtenstandards beitragen (und dadurch auch dem Aufsichtsrat von Deep Knowledge Ventures weiterhelfen) können.

a) Technikbeherrschung

[14] Eine erste Gruppe von Grundsätzen betrifft die Beherrschbarkeit und Beherrschung der eingesetzten Technik. Das WpHG verlangt beispielsweise, dass die betreffenden technischen Systeme stabil ausgestaltet sind, dass sie Vorkehrungen gegen Missbrauch enthalten, und dass Wertpapierdienstleister, die solche Systeme verwenden, die jeweiligen Algorithmen verstehen und beherrschen.⁵⁷ Ähnlich betonen die europäischen Leitlinien einerseits, dass menschlichem Handeln und menschlicher Aufsicht Vorrang gebührt, und andererseits, dass die menschlichen Akteure, die für das jeweilige technische System verantwortlich zeichnen, zugleich auch dessen Verlässlichkeit sicherstellen müssen.⁵⁸ Vergleichbare Anforderungen finden sich in den OECD-Grundsätzen.⁵⁹ Vorstandsmitglieder, die Aufgaben an KI delegieren, müssen sich demnach mit der Funktionsweise der eingesetzten Technologie vertraut machen und deren Validität ggf. in einem risikogeschützten Bereich testen. Zudem lassen sich Organisations- bzw. Betreiberpflichten ableiten, wie sie für andere Technologien, etwa die Atomenergie, längst gesetzlich normiert sind.⁶⁰ Im Fall von Vital müsste der Vorstand also dartun können, dass er entsprechende Vorkehrungen getroffen hat. Im Einzelnen ist gleichwohl schwer zu entscheiden, welches Maß an Entscheidungsautonomie der künstlichen Intelligenz mit diesem Grundprinzip vereinbar ist: Bedürfen Entscheidungen von Vital in jedem Einzelfall menschlicher Aufsicht, ist

dies nur ab einem bestimmten, etwa betragsmäßig definierten Umfang der Fall, oder reicht bereits aus, wenn die grundsätzliche Investitionsstrategie von den menschlichen Vorstandsmitgliedern entschieden wird?⁶¹

b) Auskunftspflicht

[15] Zweitens bedarf es der Offenlegung der technischen Vorgänge, damit sich diese nachprüfen und rückverfolgen lassen. Das WpHG statuiert entsprechende Anzeigepflichten. EU-Leitlinien und OECD-Grundsätze verlangen über Protokollierung und Dokumentation hinaus, dass sich die algorithmischen Entscheidungsvorgänge gegenüber den beteiligten Personen verständlich erklären lassen.⁶² Auf dieser Grundlage lässt sich die Auskunftspflicht des Vorstands konkretisieren: Er muss nicht nur die Kernparameter gem. Art. 13 II lit. f DSGVO offenlegen, also aussagekräftige Informationen über die involvierte Logik sowie über Tragweite und angestrebte Auswirkungen liefern.⁶³ Er muss darüber hinaus auch nachvollziehbar darlegen können, wie Vital zu den fraglichen Entscheidungen kommen konnte, etwa indem er die „zugefütterten“ Daten und deren Auswirkung erläutert. Die Leitlinien postulieren insgesamt eine sehr weitreichende Rechenschaftspflicht für KI-Systeme, die ein hohes Maß an Verantwortlichkeit für KI-Systeme sowie deren Nachprüfbarkeit einfordert.⁶⁴

c) Wahrung von Individualrechten

[16] Die Tendenz von Vital, bei Investitionsentscheidungen nach Hautfarbe und Geschlecht zu unterscheiden

⁵⁴ Näher, auch zum Folgenden: Braegelmann/Kaulartz/Möslein, *Rechtshandbuch Artificial Intelligence und Machine Learning*, 509 (516 ff.).

⁵⁵ In diesem Sinne, anknüpfend an Möslein ZIP 2018, 204 (211); Linardatos ZIP 2019, 504 (508); Wagner BB 2018, 1097 (1099); Weber/Kiefner/Jobst NZG 2018, 1131 (1135); anders hingegen: Becker/Pordzik ZfPW 2020, 334, 351; Zetsche AG 2019, 1 (8).

⁵⁶ Vgl. nochmals Braegelmann/Kaulartz/Möslein, *Rechtshandbuch Artificial Intelligence und Machine Learning*, 509 (517).

⁵⁷ Näher Jaskulla BKR 2013, 221 (230 f.); Kindermann/Coridaß ZBB 2014, 178 (180-183); Kobbach BKR 2013, 233 (237 f.); Schultheiß WM 2013, 596 (601).

⁵⁸ COM(2019) 168 final, 5 f. (Kernanforderungen Nr. I und II).

⁵⁹ OECD-Empfehlung (Fn. 5), unter 1.2. und 1.4.

⁶⁰ S. dazu statt aller Spindler, *Unternehmensorganisationspflichten*, 2001, S. 17–41.

⁶¹ Nach Auffassung der Europäischen Kommission dürfte Gesamtsteuerung durch den Menschen grundsätzlich ausreichen: COM(2019) 168 final, 5 (bes. Fn. 13: Dass „in jeden Entscheidungszyklus des Systems ein Mensch eingebunden sein muss“, sei „in vielen Fällen weder möglich noch wünschenswert“).

⁶² COM(2019) 168 final, 6 (Kernanforderung Nr. IV); OECD-Empfehlung (Fn. 5), unter 1.3. Allgemein zum Erfordernis der Erklärbarkeit von Algorithmen Kroll et al. U. Pa. L. Rev. 165 (2016/17), 633; in der deutschen Diskussion etwa Bitkom e. V. (Hrsg.), *Künstliche Intelligenz – Wirtschaftliche Bedeutung, gesellschaftliche Herausforderungen, menschliche Verantwortung*, 2017, 128 („Eine generelle Offenlegungspflicht von Algorithmen, auf denen Geschäftsmodelle beruhen, ist auch vor dem Hintergrund der Verbraucherinteressen äußerst problematisch“); Drexl ZUM 2017, 529 (541 f.).

⁶³ Vgl. dazu Ebers/Heinze/Krügel/Steinrötter/Möslein, *Künstliche Intelligenz und Robotik*, § 13, Rdn. 29.

⁶⁴ Ausführlicher Braegelmann/Kaulartz/Möslein, *Rechtshandbuch Artificial Intelligence und Machine Learning*, S. 509, 518 f.

den, erscheint unter Gesichtspunkten der Diskriminierung fragwürdig, ohne allerdings von vorneherein gesetzwidrig zu sein: Sie kollidiert weder mit dem aktienrechtlichen Gleichbehandlungsgrundsatz des § 53 a AktG, weil sie keine Ungleichbehandlung der eigenen Aktionäre zur Folge hat, und sie verstößt nicht gegen § 19 I des Allgemeinen Gleichbehandlungsgesetzes (AGG), weil Investitionsentscheidungen keine Massengeschäfte betreffen und auch keinen Bezug auf den Zugang zu und die Versorgung mit Gütern und Dienstleistungen haben, die der Öffentlichkeit zur Verfügung stehen. Die algorithmenspezifische Regel des WpHG statuiert ebenfalls keine einschlägigen Gleichbehandlungspflichten. Etwas ganz anderes gilt allerdings für die diversen KI-Leitlinien, die zahlreiche Prinzipien zur Wahrung von Individualrechten statuieren. Während die OECD-Grundsätze insoweit „Freiheit, Würde und Selbstbestimmung, Schutz der Privatsphäre und Datenschutz, Nichtdiskriminierung und Gleichbehandlung [...] und international anerkannte Arbeitsrechte“ aufzählen,⁶⁵ konzentriert sich die EU-Kommission auf „Privatsphäre und Datenqualitätsmanagement“ sowie „Vielfalt, Nichtdiskriminierung und Fairness“.⁶⁶ Mit dieser Forderung statuieren die Regelwerke eine Pflicht, datenbasierte Verzerrungen zu vermeiden.⁶⁷ Diese Pflicht hat der Vorstand von Deep Knowledge Ventures verletzt, indem er die diskriminierenden Entscheidungen von Vital zugelassen hat. Ob er gesetzwidrig gehandelt hat, ist damit freilich noch nicht gesagt, weil im Gegensatz zu Überwachungs- und Auskunftspflicht spezifische gesetzliche Anknüpfungspunkte fehlen.

d) Gemeinwohlverpflichtungen

[17] Ähnliches gilt schließlich hinsichtlich der Entscheidung, in ein Unternehmen zu investieren, das fragwürdige Tierversuche durchführt. Anders als vielleicht die Tierversuche selbst dürfte jedenfalls das Investment nicht gegen geltendes Recht verstoßen. Allerdings postulieren wiederum die Regelwerke von OECD und EU Gemeinwohlverpflichtungen von KI-Systemen, mit denen solche Entscheidungen möglicherweise unvereinbar sind. In den OECD-Grundsätzen heißt es beispielsweise, die Beteiligten sollten sich „proaktiv für eine verantwortungsvolle Steuerung vertrauenswürdiger KI einsetzen, die darauf abzielt, einen Nutzen für die Menschen und den Planeten zu erzielen [...] und damit ein inklusives Wachstum, eine nachhaltige Entwicklung und die Lebensqualität zu fördern“.⁶⁸ Gleichsinnig fordert die Kommission die Förderung der Nachhaltigkeit und ökologischen Verantwortlichkeit von KI-Systemen sowie die Berücksichtigung ihrer gesamtgesellschaftlichen und sozialen Auswirkungen.⁶⁹ So vage diese Programmsätze formuliert sind, so weit reichen ihre potentiellen Auswirkungen: Muss der Vorstand beim unternehmerischen Einsatz von KI-Systemen sicherstellen, dass ökologische Erwägungen Vorrang vor dem Ziel der Ge-

winnmaximierung zukommt?⁷⁰ Eine solche Verpflichtung beträfe nicht weniger als die grundlegende Ausrichtung unternehmerischer Vorstandsentscheidungen, die unter dem Schlagwort Shareholder- bzw. Stakeholder-Value kontrovers diskutiert wird.⁷¹

3. Intensität

[18] Die einzelnen Vorstandspflichten, die sich aus jenen unterschiedlichen Rechtserkenntnisquellen entfalten lassen, werfen die Frage nach der Intensität der Pflichtbindung auf. Immerhin genießt der Vorstand bei seinen Entscheidungen gem. § 93 I 2 AktG breites unternehmerisches Ermessen, das sich gerichtlicher Nachprüfung grundsätzlich entzieht.⁷² Insbesondere genießt er Organisationsermessen. Er ist daher im Grundsatz frei, Entscheidungen zu delegieren, auch auf Algorithmen.⁷³ Seine Grenze findet dieses Ermessen jedoch in normativen Vorgaben: Die Pflicht, sich bei der Amtsführung gesetzestreu zu verhalten, zählt zu den „Kardinalpflichten“.⁷⁴ Allerdings ist umstritten, ob sich diese Legalitätspflicht strikt auf gesetzliche Vorgaben beschränkt, oder ob sie umgekehrt auch im Falle von Pflichten gilt, die nicht positiv-rechtlich normiert sind, sondern (ausschließlich) ethische Verhaltensmaßstäbe verkörpern. Auch wenn teils eine Pflicht der Vorstandsmitglieder postuliert wird, allgemein anerkannte Grundsätze der Geschäftsmoral einzuhalten,⁷⁵ ist insoweit Zurückhaltung geboten, weil die „moderne Privatrechtsordnung (...) moralische Wertungen nur wohl dosiert und mittelbar über die Generalklauseln der §§ 138, 242 BGB in die bürgerlich-rechtliche Beurteilung einfließen“ lässt.⁷⁶

[19] Die Grenzlinie zwischen Gesetzesvorgaben, die der Vorstand qua dieser Legalitätspflicht strikt zu befolgen hat, und ethisch-moralischen Wertungen, die sein Ermessen nicht gleichermaßen beschränken,⁷⁷ gerät

⁶⁵ OECD-Empfehlung (Fn. 5), unter 1.2.a).

⁶⁶ COM(2019) 168 final, 6 f. (Kernforderungen III. und V.).

⁶⁷ COM(2019) 168 final, 7 (Kernforderung V.); s. außerdem nochmals Braegemann/Kaulartz/Möslein, Rechtshandbuch Artificial Intelligence und Machine Learning, 509 (519).

⁶⁸ OECD-Empfehlung (Fn. 5), unter 1.1.

⁶⁹ COM(2019) 168 final, 7 (Kernforderung VI.).

⁷⁰ Mit ähnlicher Stoßrichtung der Aktionsplan der EU-Kommission zur Finanzierung nachhaltigen Wachstums, COM(2018) 97 final vom 18.3.2018; dazu näher Möslein/Mittwoch WM 2019, 481.

⁷¹ Zu dieser Debatte demnächst umfassend: Mittwoch, Nachhaltigkeit und Unternehmensrecht, Habilitation Marburg 2020, Kapitel 5.

⁷² Vgl. MüKoAktG/Spindler § 93 Rn. 48-53; KKAktG/Mertens/Cahn § 93 Rn. 32-35; Hüffer/Koch AktG § 93 Rn. 20-22.

⁷³ Dazu ausführlich Möslein, in: Braegemann/Kaulartz (Hrsg.), Rechtshandbuch Artificial Intelligence und Machine Learning, S. 509, 511 ff.

⁷⁴ So Spindler/Stilz/Fleischer, AktG § 93 Rn. 14; s. bspw. auch LG Stuttgart, NZG 2018, 665, 676.

⁷⁵ In diesem Sinne etwa KKAktG/Mertens/Cahn, 3. Aufl. 2010, § 93, Rn. 71; Kreuzer/Schlechtriem, Die Haftung der Leitungsorgane von Kapitalgesellschaften, 1991, 9 (21); Thümmel, Persönliche Haftung von Managern und Aufsichtsräten, 5. Aufl. 2016, Rn. 184.

⁷⁶ Spindler/Stilz/Fleischer AktG § 93 Rn. 25.

⁷⁷ Allgemein zur Schwierigkeit solcher Unterscheidungen: Baum/Bälz/Dernauer/Möslein, Self Regulation in Private Law in Japan and Germany, 2018, 83.

bei KI-spezifischen Pflichten jedoch auf den Prüfstand, weil die normativen Vorgaben heterogen sind: Die Einzelpflichten konkretisieren die gesetzliche Vorgabe des § 91 II AktG, basieren in ihrer konkreten Ausgestaltung aber auf Rechts(erkenntnis)quellen, die teils (quasi-)gesetzlicher Natur sind, teils lediglich unverbindlichen Charakter haben und sich teils auch aus beiden Quellen ableiten lassen. Eine solch breite Basis hat beispielsweise die Pflicht zur Technikbeherrschung, die sich sowohl auf eine Analogie zum WpHG als auch auf die beiden KI-Leitlinien stützen kann.⁷⁸ Angesichts dieser Überlagerung unterschiedlicher Normschichten verschwimmt die Unterscheidung zwischen strikter Legalitätspflicht und breitem unternehmerischem Ermessen. Die Intensität der Pflichtbindung variiert in Abhängigkeit der jeweiligen normativen Grundlage, allerdings eher graduell: Sie ist umso größer, je stärker die fragliche Pflicht normativ verankert und je expliziter sie ausformuliert ist.⁷⁹ Bei den Anforderungen, die alleine in den rechtlich unverbindlichen KI-Leitlinien Ausdruck finden (insbesondere Wahrung von Individualrechten sowie Gemeinwohlverpflichtung) ist sie entsprechend gering. Im Gegensatz zu ungeschriebenen Grundsätzen der Geschäftsmoral sind jedoch selbst diese Pflichten vergleichsweise stark verrechtlicht: Sie sind nicht nur schriftlich niedergelegt, sondern erheben supranationalen, teils globalen Anspruch und genießen multilaterale Rückendeckung seitens staatlicher Regierungen.⁸⁰ Viel spricht dafür, dass diese Pflichten im Rahmen der Konkretisierung gesetzlicher Vorgaben eine gewisse, freilich nur mittelbare Bindungswirkung entfalten werden.⁸¹ Der Vorstand von Deep Knowledge Ventures muss durchaus befürchten, vom Aufsichtsrat in die Pflicht genommen zu werden.

V. Fazit

[20] Das Gesellschaftsrecht, das unser Fallbeispiel regelt, dient letztlich nur zur Illustration der grundlegenden und zugleich übergreifenden Überlegung, welchen rechtlichen Stellenwert ethische KI-Leitlinien haben und welche rechtlichen Folgen deren Nichteinhaltung mithin nach sich zieht.⁸² Die gleiche Frage stellt sich beispielsweise im Vertrags- und Deliktsrecht, wo Generalklauseln wie §§ 138 und 826 BGB Einfallstore ethisch-sittlicher Wertungen sind.⁸³ Rechtliche Relevanz ethischer KI-Leitlinien ist hier gleichermaßen denkbar, bereitet wegen deren heterogenem Charakter aber ebenfalls Schwierigkeiten. Die Leitlinien sind eben weder ausschließlich faktischer noch ausschließlich normativer Natur: Sie entspringen (vorerst) nicht tatsächlicher Übung, sondern der Normvorstellung von Expertengremien und inter- bzw. supranationalen Organisationen. Gleichwohl erheben sie vordergründig nicht den Anspruch, Bindungswirkung zu entfalten, sondern sind ausdrücklich als „unverbindliche“ Leitlinien konzipiert⁸⁴ und nicht in Form von Rechtsakten

gegossen. Nichtsdestotrotz lassen sie zumindest mittelbare Bindungswirkung erwarten, weil und soweit sie mit dem geltenden Recht zusammenwirken, indem sie dieses teils replizieren, teils konkretisieren. Im KI-Weißbuch der EU-Kommission heißt es denn auch, die Rückmeldungen zu den ethischen Leitlinien hätten vor allem ergeben, „dass einige ihrer Anforderungen bereits Eingang in geltende Rechts- und Verwaltungsvorschriften gefunden“ hätten.⁸⁵ Zu erwarten steht eine noch breitere, im Einzelnen aber schwer vorhersehbare und eher beliebige Einwirkung in das geltende Recht. Dass völlige Unverbindlichkeit ohnehin nicht beabsichtigt ist, klang schon in der Mitteilung an, in der die Kommission „leicht zugängliche Mechanismen“ forderte, um „angemessenen Rechtsschutz zu gewährleisten“.⁸⁶

[21] Die KI-Leitlinien liefern somit nicht nur ein Musterbeispiel für die bereits in anderen Zusammenhängen konstatierte Ethisierung des Rechts,⁸⁷ sondern lassen zugleich eine Verrechtlichung ihrer eigentlich ethischen Grundsätze erwarten. Das Verhältnis von Ethik und Recht ist vor diesem Hintergrund neu zu vermessen. Die prinzipielle Trennung von Recht und Moral, die seit *Kant* als verbindlich gegolten hatte, erfährt weitere Aufweichung.⁸⁸ Um noch einmal auf *Georg Jellinek* zurückzukommen, erscheint dieses Verhältnis jedenfalls komplexer, als in dessen berühmter Formulierung vom Recht als dem ethischen Minimum zum Ausdruck kommt.⁸⁹ Das Recht, so schrieb *Jellinek*, verhalte sich „wie der Theil zum Ganzen, wie das Fundament zum Gebäude“.⁹⁰ Auf dem Gebiet der Künstlichen Intelligenz sind dieses Fundament des Rechts und jenes Gebäude der Ethik durch zahlreiche korrespondierende Röhren eng miteinander verbunden – nicht zuletzt, weil das Gebäude primär aus offiziellen Leitlinien erbaut wird.

⁷⁸ Braegelman/Kaulartz/Möslein, Rechtshandbuch Artificial Intelligence und Machine Learning, 509 (520 f.).

⁷⁹ S. nochmals ebda.

⁸⁰ Möslein Audit Committee Quarterly II/2019, 16 (17).

⁸¹ Braegelman/Kaulartz/Möslein, Rechtshandbuch Artificial Intelligence und Machine Learning, 509 (520 f.).

⁸² Übergreifender demnächst *Möslein/IM. Horn*, Emerging Rules on Artificial Intelligence, in: Durovic/ Di Matteo/ Ortolani u. a. (Hrsg.), *Lawyering in the Digital Age*, in Vorb. f. 2020

⁸³ Zur Diskussion um die Öffnung der Privatrechtsordnung gegenüber solchen Wertungsprinzipien vgl. etwa *Auer*, Materialisierung, Flexibilisierung, Richterfreiheit, 2005, S. 139; *Staudinger/Rieble*, 2017, § 138, Rn. 62 f.; auf europäischer Ebene *Riesenhuber/Möslein/Röthel*, Europäische Methodenlehre, 2. Aufl. 2020, § 11, Rdn. 42-44; speziell für das Wirtschaftsrecht *Reuter ZGR* 1987, 489.

⁸⁴ *Europäische Kommission* (Fn. 7), COM (2019), 168 final., S. 4.

⁸⁵ *Europäische Kommission* (Fn. 7), COM (2020) 65 final., S. 11.

⁸⁶ *Europäische Kommission* (Fn. 7), COM (2019), 168 final., S. 8.

⁸⁷ Vgl. Nachw. Fn. 10; s. auch *Paulus/Schneider* Jura 2013, 1197.

⁸⁸ Zu diesem Prozess neben den Nachw. Vorn. auch *Wegerich* Die Flucht in die Grenzenlosigkeit, 2004, S. 114.

⁸⁹ *G. Jellinek*, Die sozialetische Bedeutung von Recht, Unrecht und Strafe, 1878, S. 42.

⁹⁰ Ebda., S. 43; vgl. demgegenüber *G. Schmoller*, Grundriß der Allgemeinen Volkswirtschaftslehre, 1. Teil 1920, S. 57 („ethisches Maximum“); ebenso *A. Kaufmann*, Rechtsphilosophie, 2. Aufl. 1997, S. 216.

Prof. Dr. Thomas Riehm*

Nein zur ePerson!

Gegen die Anerkennung einer digitalen Rechtspersönlichkeit

Seit über zehn Jahren schon wird in Rechtswissenschaft und Politik diskutiert, ob Systeme Künstlicher Intelligenz als rechtsfähige digitale Rechtssubjekte („ePerson“) behandelt werden sollen. Der nachfolgende Beitrag untersucht diese Frage im Hinblick auf die Zuerkennung zivilrechtlicher Rechtsfähigkeit an KI-Systeme und gelangt zu dem Ergebnis, dass dies weder *de lege lata* möglich noch *de lege ferenda* wünschenswert ist.

I. Einleitung

[1] Die Vorstellung einer „digitalen Rechtspersönlichkeit“ ist beinahe so alt wie die Vorstellung von künstlicher Intelligenz selbst: Schon die „Roboter Gesetze“ des Science-Fiction-Autors *Isaac Asimov*¹ aus dem Jahr 1950 sahen die Roboter selbst als Adressaten, also als Träger von Rechten und Pflichten, mithin als rechtsfähige Rechtssubjekte – nicht etwa die Menschen, die die Roboter konstruieren oder betreiben. Was als Vorstellung in der Science-Fiction anfang, wird seit über zehn Jahren auch in der Rechtswissenschaft und in der Politik diskutiert – z. T. *de lege ferenda*², z. T. sogar *de lege lata*.³

[2] Anfang 2017 hat sogar das Europäische Parlament vorgeschlagen, „langfristig einen speziellen rechtlichen Status für Roboter zu schaffen, damit zumindest für die ausgeklügelten autonome Roboter ein Status als elektronische Person festgelegt werden könnte, die für den Ausgleich sämtlicher von ihr verursachten Schäden verantwortlich wäre [...]“.⁴ Diese Vorschläge sind allerdings von der Kommission nicht aufgegriffen worden.⁵

[3] Ein Grund für die Vorstellung einer „ePerson“ dürfte darin liegen, dass KI-Systeme häufig humanoid dargestellt werden, was eine menschenähnliche Behandlung im Recht intuitiv nahelegt. Freilich genügt dies ebenso wenig als Begründung, warum die Rechtsordnung ein derartiges System als rechtsfähig anerkennen sollte, wie der Umstand, dass Menschen für KI-Systeme Empathie empfinden.⁶ Andernfalls müssten selbst Tiere als rechtsfähig angesehen werden, was jedenfalls für die zivilrechtliche Rechtsfähigkeit nicht ernsthaft vertreten wird. Um KI-Systeme als rechtsfähig zu behandeln, bedarf es vielmehr nicht einer empirischen oder moralischen, sondern einer spezifisch rechtlichen Begründung.⁷

[4] Der vorliegende Beitrag klammert die (rechts)philosophische Diskussion um die „(Rechts)Persönlich-

keit“ von KI-Systemen⁸ bewusst ebenso aus wie die Debatte um die verfassungsrechtliche Grundrechts-

* Der Autor ist Inhaber des Lehrstuhls für Deutsches und Europäisches Privatrecht, Zivilverfahrensrecht und Rechtstheorie an der Universität Passau, Sprecher des dortigen Instituts für das Recht der digitalen Gesellschaft (IRDG) und einer der geschäftsführenden Herausgeber der RD. Der Beitrag beruht auf Vorträgen des Autors an den Universitäten Bonn, Speyer und Frankfurt sowie auf seinem Kap. 6.1 in *Kaulartz/Braegelmann, Rechtshandbuch Artificial Intelligence und Machine Learning*, 2020, das im Folgenden nicht im Einzelnen nachgewiesen wird. Sämtliche Internetquellen wurden zuletzt am 27.10.2020 abgerufen.

- 1 Diese lauten (s. *Asimov, Ich, der Robot*, 1952, 1): „Das nullte Gesetz: Ein Roboter darf der Menschheit keinen Schaden zufügen oder durch Untätigkeit zulassen, dass der Menschheit ein Schaden zugefügt wird. Das erste Gesetz: Ein Roboter darf einem menschlichen Wesen keinen Schaden zufügen oder durch Untätigkeit zulassen, dass einem menschlichen Wesen Schaden zugefügt wird, es sei denn, dies würde das nullte Gesetz der Robotik verletzen. Das zweite Gesetz: Ein Roboter muss dem ihm von einem menschlichen Wesen gegebenen Befehl gehorchen, es sei denn, dies würde das nullte oder das erste Gesetz der Robotik verletzen. Das dritte Gesetz: Ein Roboter muss seine Existenz beschützen, es sei denn, dies würde das nullte, das erste oder das zweite Gesetz der Robotik verletzen.“
- 2 Zuerst wohl *Matthias, Automaten als Träger von Rechten*, 2007; *Gitter, Softwareagenten im elektronischen Geschäftsverkehr*, 2008; aus jüngerer Zeit etwa *Mayinger, Die künstliche Person*, 2017.
- 3 *Wettig, Vertragsschluss mittels elektronischer Agenten*, 2010; für Teilrechtsfähigkeit *de lege lata Teubner AcP* 218 (2018), 155 ff.; *Schirmer JZ* 2016, 660 ff.; *ders. JZ* 2019, 711 ff.; *Specht/Herold MMR* 2018, 40 ff.
- 4 *EU-Parlament, Entschließung vom 16. Februar 2017 mit Empfehlungen an die Kommission zu zivilrechtlichen Regelungen im Bereich Robotik*, 2015/2103(INL), Ziff. 59 f); s. dazu krit. *Lobmann ZRP* 2017, 168 ff.; *High Level Expert Group on Artificial Intelligence, Liability for Artificial Intelligence*, 2019, S. 6, 36 f., abrufbar unter: <https://beck-link.de/r6nme>.
- 5 *EU-Kommission, Schaffung von Vertrauen in eine auf den Menschen ausgerichtete künstliche Intelligenz*, COM(2019) 168 final.
- 6 Aus der Verhaltensforschung s. *Nijssen/Müller/van Baaren u. a. Social Cognition* 37 (2019), 41 ff.
- 7 Ähnlich auch *Beck AJP* 2017, 183 (185, 187 ff.).
- 8 S. dazu etwa *Kluge/Müller InTeR* 2017, 24 ff.; *Teubner AcP* 218 (2018), 155 ff.; *Bora, Kommunikationsadressen als digitale Rechtssubjekte*, 1.10.2019, abrufbar unter: <https://beck-link.de/fc6hk>; *Misselhorn, Digitale Rechtssubjekte, Handlungsfähigkeit und Verantwortung aus philosophischer Sicht*, 2.10.2019, abrufbar unter: <https://beck-link.de/b6xta>; *Günther/Hilgendorf/Beck, Robotik und Gesetzgebung*, 2013, 239 ff.; *dies. AJP* 2017, 183 ff.; zusammenfassend *Schulz, Verantwortlichkeit bei autonom agierenden Systemen*, 2015, 91 ff.

fähigkeit⁹ und die Strafmündigkeit,¹⁰ und behandelt ausschließlich die Frage ihrer zivilrechtlichen Rechtsfähigkeit, also der Fähigkeit, Träger zivilrechtlicher Rechte und Pflichten zu sein und ein Vermögen zu haben.¹¹ Diese ist unstrittig unabhängig davon, ob das betreffende Rechtssubjekt ein Mensch ist oder nicht, wie die Existenz juristischer Personen und rechtsfähiger Personengesellschaften belegt. Ebenso unstrittig ist, dass die zivilrechtliche Rechtsfähigkeit nicht apriorisch vorgegeben ist, sondern zur Disposition des Gesetzgebers steht.¹²

II. Ausgangspunkt: Die „Verantwortungslücke“

[5] Aus zivilrechtlicher Sicht liegt der wesentliche Grund für die Forderung nach der Anerkennung einer digitalen Rechtspersönlichkeit („ePerson“) in der Befürchtung, dass andernfalls eine „Verantwortungslücke“ auftritt.¹³ Diese Befürchtung findet sich sowohl im Vertragsrecht als auch im Haftungsrecht; sie speist sich jeweils aus Erwägungen, welche die Zurechnung des „Verhaltens“ eines KI-Systems zu seinem Betreiber lockern sollen. Begründet wird dies jeweils mit der fehlenden Kontrolle des Betreibers über das System: Diesem solle nicht das „Autonomierisiko“, also das Risiko unvorhersehbarer Handlungen des Systems,¹⁴ auferlegt werden.

[6] So finden sich in der Rechtsgeschäftslehre Ansätze, die Erklärungen von KI-Systemen dem Betreiber nicht unmittelbar als eigene Willenserklärungen zuzurechnen,¹⁵ indem die Systeme entweder als Boten (mit der Anfechtungsmöglichkeit nach § 120 BGB) oder gar als Stellvertreter i. S. v. §§ 164 ff. BGB (mit der Möglichkeit einer gegenüber Dritten wirksamen Beschränkung der Vertretungsmacht)¹⁶ angesehen werden. Im Bereich der außervertraglichen Haftung ergibt sich eine „Verantwortungslücke“ aus einer Anwendung des in § 823 I BGB verankerten Verschuldensprinzips, wonach der Betreiber nur haftet, wenn ihm selbst eine Verkehrspflichtverletzung im Hinblick auf die Überwachung des Systems oder auf die Abwehr der von diesem ausgehenden Gefahren nachgewiesen werden kann.¹⁷ Je unvorhersehbarer das Verhalten des KI-Systems ist, desto eher scheidet eine solche Verkehrspflichtverletzung aus, eben weil der Betreiber auch das Fehlverhalten nicht vorhersehen konnte.¹⁸

[7] Ein Parallelproblem tritt schließlich bei der vertraglichen Schadensersatzhaftung nach §§ 280 ff. BGB auf, wenn das „Verhalten“ des KI-Systems dem Schuldner nicht nach § 278 BGB zugerechnet wird:¹⁹ Auch dann würde eine Haftung des Schuldners ausscheiden, wenn dieser sich im Hinblick auf sein persönliches Verschulden exkulpieren kann (§ 280 I 2 BGB).²⁰

[8] Würde der Betreiber anstelle des KI-Systems Menschen einsetzen, würde jeweils eine Eigenhaftung der Hilfsperson an die Stelle der „Verantwortungslücke“ treten: bei der Stellvertretung²¹ die Haftung des Vertreters ohne Vertretungsmacht (§ 179 I BGB),²² bei der deliktischen Haftung die Eigenhaftung des Gehilfen aus § 823 I BGB. Bei der vertraglichen Schadensersatzhaftung würde die „Verantwortungslücke“ wegen der unmittelbaren Zurechnung des Fehlverhaltens der Hilfsperson gem. § 278 BGB gar nicht erst auftreten.²³ Erst die Eigenhaftung der Hilfsperson bzw. die Zurechnung über § 278 BGB machen das System der vertraglichen und außervertraglichen Haftung beim Einsatz menschlicher Hilfspersonen komplett. Die Alternative bestünde darin, das Autonomierisiko dem jeweils betroffenen Dritten – Vertragspartner oder Geschädigter – aufzuerlegen; das kann freilich nicht gewünscht sein.

[9] Sobald man also KI-Systeme wie autonome Hilfspersonen behandelt und dementsprechend die Zurechnung ihrer „Handlungen“ an den Betreiber lockert, folgt daraus der Bedarf nach einer Eigenhaftung des KI-Systems, welche wiederum dessen Rechtsfähigkeit und die Existenz einer Haftungsmasse voraussetzt. Vor diesem Hintergrund sind die verschiedenen Versuche in der Literatur verständlich, die Rechtsfähigkeit autonomer KI-Systeme zu begründen.

9 S. dazu v. a. *Ingold* Der Staat 53 (2014), 193 ff.; *Bull*, Sinn und Unsinn des Datenschutzes, 2015, 120; *Kersten* JZ 2015, 1 (7 f.); *ders.* ZfRSoz 37 (2017), 8 ff.; *Joerden/Hilgendorf/Thiele/Fitzi/Matsuzaki*, Menschenwürde und Medizin, 2013, 919 ff.

10 Hierzu *Beck* JR 2009, 225 (229 f.); *Beck/Hilgendorf*, Jenseits von Mensch und Maschine, 2012, 119 (128 ff.); *Hilgendorf/Hötitzsch/Hilgendorf*, Das Recht vor den Herausforderungen der modernen Technik, 2013, 11 (29 f.); *Günther*, Roboter und rechtliche Verantwortung, 2016, 246 ff.; *Yuan* RW 9 (2018), 477 ff.

11 Zur Unterscheidung zwischen Rechtspersönlichkeit und Rechtsfähigkeit *Lehmann* AcP 207 (2007), 225 (240).

12 *Lohsse/Schulze/Staudenmayer/Wagner*, Liability for Artificial Intelligence and the Internet of Things, 2019, 27 (55); *Beck* AJP 2017, 183 (186).

13 Eingehend *Teubner* AcP 218 (2018), 155 (157 ff.); *Beck* AJP 2017, 183 (184); aus technischer Sicht *Matthias*, Automaten als Träger von Rechten, 2. Aufl. 2010, 35 ff.

14 *Zech* in Ständige Deputation des deutschen Juristentages (Hrsg.), Verhandlungen des 73. Deutschen Juristentages, 2020, A 41 ff.

15 Überblick bei *Foerster* ZfPW 2019, 418 (424 ff.).

16 Näher *Günther*, Roboter und rechtliche Verantwortung, 45 ff.

17 *Seelmann/Gless/Janal*, Intelligente Agenten und das Recht, 2016, 141 (148); *Spindler* CR 2015, 766 (768); allgemein *MüKoBGB/Wagner*, BGB, 8. Aufl. 2020, § 823 Rn. 456 ff.

18 S. auch *Hilgendorf/Hanisch*, Robotik im Kontext von Recht und Moral, 2013, 27 (33 f.). Zum Ausschluss der Haftung wegen Überkomplexität der erforderlichen Schutzmaßnahmen s. *Günther*, Roboter und rechtliche Verantwortung, 124 ff.

19 Hierzu *Klingbeil* JZ 2019, 718 ff.

20 *Foerster* ZfPW 2019, 418 (431).

21 In vielen Fällen verhindert schon die Unbeschränkbarkeit der gesellschaftsrechtlichen Vertretungsmachten (§§ 37 II 1 GmbHG, 82 I AktG, 27 II 1 GenG, 126 II HGB) sowie der Schutz des guten Glaubens an den Umfang der Vertretungsmacht (§§ 173 BGB, 54 III HGB) die Entstehung einer „Verantwortungslücke“.

22 Dazu *Foerster* ZfPW 2019, 418 (426); *Grapentin*, Vertragsschluss und vertragliches Verschulden beim Einsatz von künstlicher Intelligenz und Softwareagenten, 2018, 98 ff.

23 S. hierzu auch *Günther*, Roboter und rechtliche Verantwortung, 64 ff.

III. Die These von der Rechtsfähigkeit („ePerson“)

1. Rechtsfähigkeit als Lösungsvorschlag

[10] Zur Schließung dieser Verantwortungslücke wird in der Literatur teilweise vorgeschlagen, KI-Systeme – z. T. nur *de lege ferenda*²⁴, z. T. sogar *de lege lata*²⁵ – als rechtsfähige digitale Rechtspersönlichkeiten („ePerson“) zu betrachten, die über eigenes Vermögen verfügen und selbst Adressaten rechtlicher Pflichten sein können. In der Folge sollen sie für ihre Handlungen selbst haften – anstelle ihrer Betreiber.²⁶ Dies wird für das Vertragsrecht²⁷ ebenso vorgeschlagen wie im Haftungsrecht.²⁸ Ausgangspunkt dieser Überlegungen ist – neben philosophischen²⁹ und soziologischen Erwägungen³⁰ –, dass KI-Systeme ähnlich wie menschliche Gehilfen im Detail unberechenbar und nicht vollständig kontrollierbar sein können.³¹ Eine konsequente Fortführung der Gleichstellung von KI-Systemen mit menschlichen Gehilfen führt geradewegs zum Postulat ihrer Rechtsfähigkeit, um die vorstehend beschriebene Eigenhaftung des Gehilfen bzw. Stellvertreters realisieren zu können. KI-Systeme würden so zu tauglichen Adressaten von Haftungsnormen und Schuldner von Schadensersatzansprüchen, die auch über eigenes Haftungsvermögen verfügen könnten.

[11] Damit ist allerdings zugleich die Frage angesprochen, mit welchem Vermögen eine solche digitale Rechtspersönlichkeit ausgestattet sein sollte. Denn ohne Haftungsmasse ist eine Eigenhaftung des KI-Systems sinnlos.³² Selbst wenn die Haftung über eine Pflicht-Haftpflichtversicherung des Systems gelöst werden sollte,³³ müssten deren Beiträge aus einem Vermögen des Systems finanziert werden. Dementsprechend wären Regeln über die Mindestkapitalausstattung von KI-Systemen erforderlich – die entweder vom Hersteller, vom Verkäufer oder vom Betreiber einzuzahlen wäre,³⁴ wirtschaftlich über die Preisgestaltung aber immer letzteren treffen würde.

2. Kritik

[12] Ein derart radikaler Eingriff in die Grundstrukturen des Privatrechts, wie er mit der Anerkennung einer neuen Art von Rechtssubjekten verbunden ist, setzt allerdings eine umfassende Analyse seiner rechtsdogmatischen Folgewirkungen voraus.

a) Wozu Rechtsfähigkeit?

[13] Aus zivilrechtlicher Sicht ist die zentrale Funktion der Schaffung eines Rechtssubjekts die Trennung verschiedener Vermögensmassen: Die natürlichen Personen, die die Entität betreiben, werden durch die An-

erkennung seiner Rechtsfähigkeit von der Haftung für die Folgen des Handelns dieser Entität befreit – zugunsten der Haftung des Rechtssubjekts. Zweck einer solchen Haftungsbeschränkung ist es üblicherweise, das Eingehen von – gesamtwirtschaftlich erwünschten – Risiken zu fördern, indem diese auf die Gläubiger des Rechtssubjekts abgewälzt werden.³⁵ Zudem führt die Anerkennung der Rechtsfähigkeit zu einer Bündelung von Rechten und Pflichten sowie Aktiva und Passiva bei der Entität, sowie dazu, dass sie für die Folgen „ihrer“ (d. h. der ihr zugerechneten) Handlungen auch rechtlich einstehen muss.³⁶ Damit ist zugleich sichergestellt, dass Chancen und Risiken eines Verhaltens das gleiche Subjekt treffen, sodass dieses einen Anreiz erhält, sein „Verhalten“ so zu steuern, dass es nur solche Risiken eingeht, denen mindestens gleichwertige Chancen gegenüberstehen.

[14] Erst dieser Zusammenhang führt auch dazu, dass das Rechtssubjekt für die Rechtsordnung steuerbar wird, weil es dann die Konsequenzen eines Verstoßes selbst tragen muss: Im Wege der Haftung für rechtswidrig verursachte Schäden sowie ggfs. auch im Wege von Bußgeldern oder Geldstrafen. Aus zivilrechtlicher Sicht ist die Vermögenshaftung für verursachte Schäden die zentrale Voraussetzung für eine Verhaltenssteuerung mithilfe des Haftungsrechts.

b) Abgrenzungsprobleme

[15] Die Anerkennung von KI-Systemen als rechtsfähig setzt voraus, dass sie eindeutig identifizierbar sind: Jedes Rechtssubjekt muss nach außen als solches erkennbar

²⁴ Günther, Roboter und rechtliche Verantwortung, 251 ff.; Wettig, Vertragsschluss mittels elektronischer Agenten, 369 ff.; Mayinger, Die künstliche Person, 166 ff.; Matthias, Automaten als Träger von Rechten.

²⁵ Wettig, Vertragsschluss mittels elektronischer Agenten.

²⁶ Schon früh – im Zusammenhang mit elektronischen Agenten – Wein 6 [Fall] Harv. J. Law & Tec 103 (111 ff.) (1992); ähnlich auch schon Allen/Widdison 9 Harv. J. Law & Tec 25 (28 f.) (1996) Aus neuerer Zeit s. Wettig/Zehender, The Electronic Agent: A Legal Personality under German Law?, 2003, sub IV.2., abrufbar unter: <https://beck-link.de/kc3tt>.

²⁷ Matthias, Automaten als Träger von Rechten, passim.

²⁸ Mayinger, Die künstliche Person, 80 ff., 229 f.

²⁹ S. etwa Hubbard Temp. L. Rev. 83 (2011), 405 ff.; Seelmann/Gless/Erhardt/Mona, Intelligente Agenten und das Recht, 61 ff.

³⁰ S. etwa Teubner J Law & Society 33 (2006), 497 ff.; Beck AJP 2017, 183 (186 f.).

³¹ Etwa Matthias, Automaten als Träger von Rechten, 46; Beck JR 2009, 225 (229 f.); Beck/Hilgendorf, Jenseits von Mensch und Maschine, 119 (125 ff.).

³² So auch Lohsse/Schulze/Staudenmayer/Wagner, Liability for Artificial Intelligence and the Internet of Things, 27 (56); Foerster ZfPW 2019, 418 (426).

³³ Beck AJP 2017, 183 (185); s. dazu Lohsse/Schulze/Staudenmayer/Wagner, Liability for Artificial Intelligence and the Internet of Things, 27 (58 f.).

³⁴ S. auch Beck AJP 2017, 183 (189).

³⁵ Lohsse/Schulze/Staudenmayer/Wagner, Liability for Artificial Intelligence and the Internet of Things, 27 (56); Spindler CR 2015, 766 (776 f.).

³⁶ Beck Robotics and Autonomous Systems 86 (2016), 138 (sub 4. nach Fn. 35).

sein.³⁷ Diese Abgrenzung ist zum einen formeller Natur – also die Identifikation eines konkreten Subjekts und seine Unterscheidung von anderen Subjekten–, und zum anderen materieller Natur – also die Unterscheidung von KI-Systemen von anderen, nicht rechtsfähigen Programmen oder Geräten.

[16] Bereits die formelle Abgrenzung stößt auf Schwierigkeiten.³⁸ Zwar könnten KI-Systeme mit einer konkreten Verkörperung (Fahrzeuge, physische Roboter o. Ä.) anhand ihrer Körperlichkeit identifiziert werden: ein Gerät, ein Rechtssubjekt. Das wird allerdings schon zweifelhaft, wenn in einem Gerät mehrere autonome Subsysteme aktiv sind, oder wenn sich autonome Kleinroboter zu vernetzten „Roboterschwärmen“ zusammenschließen. Wenn aber KI-Systeme ohne physische Repräsentation betroffen sind (Handelsalgorithmen an der Börse, Internet-Suchmaschinen o. Ä.), ist eine solche körperliche Zuordnung ausgeschlossen, weil die Algorithmen nicht einer konkreten Hardware zugeordnet werden können. Dann müsste geklärt werden, ob der Algorithmus selbst oder eine konkret gestartete Instanz davon als rechtsfähig angesehen werden soll.³⁹ Plakativ gefragt: Wie viele „Siris“ existieren? – Auf jedem Handy eine eigene, für jeden Nutzer eine eigene, oder eine zentrale?

[17] Praktisch dürfte dieses formelle Abgrenzungsproblem nur mit einem Register nach dem Vorbild des Gesellschaftsrechts lösbar sein.⁴⁰ Wegen der großen Dynamik der Entwicklung von KI-Systemen müsste dies sinnvollerweise im Rahmen einer Blockchain dezentral organisiert werden, wo einem System je ein eigenes „wallet“ für sein Vermögen zugeordnet werden könnte. Die Eintragung in der Blockchain müsste dabei konstitutiv ausgestaltet werden, sodass die Betreiber nur dann von einer Haftungsbeschränkung profitieren können, dieses eingetragen ist.⁴¹ Mit dieser Maßgabe erscheint das formelle Abgrenzungsproblem zumindest theoretisch teilweise lösbar, auch wenn die praktischen Herausforderungen eines solchen – sinnvollerweise überstaatlichen – Registers erheblich erscheinen.

[18] In materieller Hinsicht sind diejenigen Systeme zu identifizieren, die hinreichend „autonom“ sind, um die Zuerkennung von Rechtsfähigkeit zu rechtfertigen. Bei vorhersehbaren deterministischen Algorithmen fehlt es schon an einer „Verantwortungslücke“, die durch die Anerkennung als Rechtssubjekt geschlossen werden könnte. Schließlich soll nicht jeder Taschenrechner – der auch eine einfache Form künstlicher Intelligenz darstellt⁴² – durch Eintragung in ein Register die Rechtsfähigkeit erlangen können und dadurch die Haftung seines Betreibers beschränken. Denjenigen Grad an Autonomie *rechtssicher* zu bestimmen, ab welchem von einem hinreichend autonomen System gesprochen wer-

den kann, ist allerdings kaum möglich.⁴³ Allenfalls könnte dieses Abgrenzungsproblem im Rahmen einer Registereintragung mit gelöst werden, indem vom Register selbst geprüft wird, ob das System hinreichend autonom ist, und zum anderen an die Eintragung im Register eine entsprechende Fiktion geknüpft wird. Nach welchen Maßstäben dies allerdings ein Register rechtssicher prüfen sollte, bleibt unbeantwortet und dürfte kaum lösbar sein.

c) Überlebenswille

[19] Selbst wenn man allerdings entgegen der hier vertretenen Auffassung die Abgrenzungsprobleme für lösbar hält, ist ein ganz zentrales Problem der Anerkennung der Rechtsfähigkeit von KI-Systemen bisher kaum beleuchtet: die Frage nach dem „Überlebenswillen“ des Systems. Als ungeschriebene Prämisse setzt die Zuschreibung von Rechtsfähigkeit an eine Entität nämlich voraus, dass diese den „Willen“ hat, wirtschaftlich zu überleben. Die rechtliche Verhaltenssteuerung durch Vertrags- und Haftungsrecht kann nur auf der Grundlage der Prämisse funktionieren, dass Rechtssubjekte ihr Vermögen nicht verlieren „wollen“. Nur wer sein Vermögen behalten will, befolgt rechtliche Verhaltensregeln, um finanzielle Konsequenzen von Regelverletzungen zu vermeiden. Wer dagegen gegenüber finanziellen Verlusten indifferent ist, ist für rechtliche Steuerungsmechanismen praktisch nicht ansprechbar.⁴⁴ Ein Rechtssubjekt, das an seinem eigenen wirtschaftlichen Überleben kein Interesse hat, ist zudem für die übrigen Marktteilnehmer unberechenbar und dadurch eine Gefahr für den Rechtsverkehr – wie Gerichtsvollzieher aus dem praktischen Umgang mit vermögenslosen Schuldnern, die im wirtschaftlichen Sinne nichts mehr zu verlieren haben, berichten können.

[20] Grundsätzlich verfügen Menschen natürlicherweise über einen solchen wirtschaftlichen „Überlebenswillen“. Bei ihnen können finanzielle Verluste letztlich sogar physisch existenzbedrohend sein: Wer sein Essen nicht mehr bezahlen kann, droht zu verhungern. Freilich verhindert das jedenfalls in Deutschland der moderne Sozialstaat; doch auch die Furcht vor einem Leben am pfändungsfreien Existenzminimum oder vor einer

³⁷ *Lehmann AcP* 207 (2007), 225 (247).

³⁸ *Beck AJP* 2017, 183 (190).

³⁹ S. dazu auch *Spindler CR* 2015, 766 (775).

⁴⁰ So auch *Beck AJP* 2017, 183 (190).

⁴¹ Ähnlich *Beck AJP* 2017, 183 (190).

⁴² *Bryson/Wyatt*, *Artificial Intelligence*, April 1997, abrufbar unter: <https://beck-link.de/nd6df>.

⁴³ S. dazu auch *Beck AJP* 2017, 183 (188 f.); *Seilmann/Gless/Janal*, *Intelligente Agenten und das Recht*, 141 (157); auch die Stufen des § 1 a StVG dürften hier nicht weiterhelfen, weil sie nicht mit Blick auf die Rechtsfähigkeit definiert wurden.

⁴⁴ Angedeutet bei *Lohsse/Schulze/Staudenmayer/Wagner*, *Liability for Artificial Intelligence and the Internet of Things*, 27 (57 f.).

Privatinsolvenz, selbst die vor einem Verlust des gewohnten Komforts kann genügen, damit Menschen auf finanzielle Handlungsanreize reagieren und sich rechtskonform verhalten.

[21] Dieses Problem existiert auch im Konzernrecht, wo Fälle bekannt sind, in denen eine Tochtergesellschaft einem übergeordneten Konzernzweck „geopfert“ wird, sodass deren eigener „Überlebenswille“ entfällt. Im Gesellschaftsrecht wurden verschiedenste Konstruktionen entwickelt, um in einer derartigen „Anomalie“ die Haftungsbeschränkung der „geopferten“ Gesellschaft faktisch außer Kraft zu setzen,⁴⁵ insbesondere die sogenannte Existenzvernichtungshaftung nach § 826 BGB, wonach die Geschäftsführer einer Kapitalgesellschaft persönlich haften, wenn sie die Gesellschaft vorsätzlich „geopfert“ haben.⁴⁶ In der Sache stellt sich diese Haftung als Sanktion für das Fehlen eines „Überlebenswillens“ der Gesellschaft dar, kann also als Beleg für das implizite Erfordernis eines solchen Willens dienen. Dieser stellt den Regelfall dar, weil davon ausgegangen werden darf, dass die Geschäftsführer einer Gesellschaft diese so führen werden, dass sie den Gesellschaftszweck nachhaltig verwirklichen kann.⁴⁷

[22] Im Hinblick auf KI-Systeme dürfte diese Voraussetzung die problematischste sein: Kein Algorithmus hat *per se* einen Überlebenswillen. Vielmehr sind Computer *per se* zunächst vollkommen indifferent gegenüber ihrem Vermögensstatus. Eine Verlustaversion kann ihnen selbstverständlich einprogrammiert werden; ohne eine solche Programmierung sind sie aber für mittelbare rechtliche Steuerung über finanzielle Anreize nicht ansprechbar, sodass ihnen auch keine Rechtsfähigkeit verliehen werden sollte.

[23] Wie allerdings – etwa im Rahmen eines Registrierungsverfahrens – sichergestellt werden soll, dass ein KI-System tatsächlich einen wirtschaftlichen Überlebenswillen hat und diesen trotz aller „Selbstlernfähigkeiten“ auch dauerhaft behalten wird, ist derzeit völlig schleierhaft. Wenn es gerade das Charakteristikum „autonomer“ Systeme ist, dass ihr „Verhalten“ für Betreiber nicht vorhersehbar ist, erscheint es kaum vorstellbar, dass die Grundtendenz einer Verlustaversion zuverlässig immer Teil der Optimierungsstrategien eines KI-Systems sein wird. Demnach sollte die Anerkennung von Rechtsfähigkeit von KI-Systemen jedenfalls an diesem Kriterium scheitern.

d) Stammkapital

[24] Schließlich wäre im Falle einer Anerkennung von Rechtsfähigkeit auch noch zu klären, ob und ggfs. in welcher Höhe derartige Systeme mit Stammkapital auszustatten wären. Dieses Kapital würde allerdings – anders als bei Handelsgesellschaften – nicht produktiv

eingesetzt werden, sondern stünde lediglich als totes Kapital für potenzielle Haftungsfälle bereit,⁴⁸ und wäre zudem notwendigerweise begrenzt, was wiederum den Bedarf nach einer Rückgriffhaftung des Betreibers (oder anderer) wecken würde.⁴⁹ Wesentlich sinnvoller wäre insofern, für derartige Systeme eine verpflichtende Haftpflichtversicherung vorzusehen, die zugleich das Problem der notwendigerweise beschränkten Haftungsmasse eines reinen Stammkapitals lösen würde. Wenn der Kern der Vermögenshaftung eines KI-Systems aber letztlich in einer Haftpflichtversicherung besteht, könnte diese auch beim Betreiber angesiedelt werden, sofern dieser einer verschuldensunabhängigen Haftung für vom System verursachte Schäden unterworfen wird; eine Haftung des Systems selbst und damit dessen Rechtsfähigkeit wären dann nicht mehr erforderlich.

3. Fazit

[25] Nach dem Vorstehenden sind die fundamentalen Prämissen für die Verleihung von Rechtsfähigkeit an KI-Systeme praktisch kaum jemals erfüllbar. Damit kommt eine Verleihung von Rechtsfähigkeit in der Regel nicht in Betracht. Nach dem gegenwärtigen Stand von Technik und Rechtsentwicklung ist die Verleihung von zivilrechtlicher Rechtsfähigkeit an KI-Systeme daher abzulehnen. Dementsprechend entspricht es heute der h. M., dass die Anerkennung einer Rechtsfähigkeit von KI-Systemen weder *de lege lata* möglich noch *de lege ferenda* wünschenswert ist.⁵⁰ Auf diesem Standpunkt stehen auch die Datenethikkommission der Bundesregierung⁵¹ und die High Level Expert Group on Artificial Intelligence der EU-Kommission.⁵²

IV. Die These von der Teilrechtsfähigkeit

[26] Als „milderes Mittel“ zur Überbrückung der „Verantwortungslücke“ wird in der Lit. z. T. vorgeschlagen,

⁴⁵ Roth/Altmeyden/*ders.*, GmbHG, 9. Aufl. 2019, § 13 Rn. 73 ff.

⁴⁶ BGHZ 173, 246.

⁴⁷ S. auch Grigoleit, Gesellschafterhaftung für interne Einflussnahme im Recht der GmbH, 2006, 59 f.: „Prinzip der dezentralen Gewinnverfolgung“.

⁴⁸ Gless/Janal JR 2016, 561 (571); Hilgendorf/Hanisch, Robotik im Kontext von Recht und Moral, 27 (40).

⁴⁹ High Level Expert Group on Artificial Intelligence, Liability for Artificial Intelligence, 38; Lohsse/Schulze/Staudenmayer/Koch, Liability for Artificial Intelligence and the Internet of Things, 99 (115).

⁵⁰ S. etwa Lohsse/Schulze/Staudenmayer/Koch, Liability for Artificial Intelligence and the Internet of Things, 99 (115); Faust/Schäfer/Altammer u. a./Wagner, Zivilrechtliche und rechtsökonomische Probleme des Internet und der künstlichen Intelligenz, 2019, 1 ff.; Spindler CR 2015, 766 ff.; Schaub JZ 2017, 342 (345 f.); Gless/Janal JR 2016, 561 (571); Bull, Sinn und Unsinn des Datenschutzes, 120; Riehm/Meier in DGRI Jahrbuch 2018, 2019, 1 (31); Grininger in JbZivRWiss 2019, 2020, 151 (164 f.); Zech in 73. dJt I (A 97).

⁵¹ Datenethikkommission, Gutachten, 2019, S. 219, abrufbar unter: <https://beck-link.de/z5dpe>.

⁵² High Level Expert Group on Artificial Intelligence, Liability for Artificial Intelligence, 37 ff.; s. dazu auch Open letter to the European Commission – Artificial Intelligence and Robotics (<http://www.robotics-openletter.eu/>), Ziff. 2.

KI-Systeme als „teilrechtsfähig“ zu behandeln.⁵³ KI-Systeme sollen danach nur insoweit als rechtsfähig angesehen werden, als dies für die Anwendbarkeit der Zurechnungsregeln des Stellvertretungsrechts (§ 164 I BGB) und der vertraglichen Schadensersatzhaftung (§ 278 BGB) erforderlich ist. Ausdrücklich wird etwa die Einführung eines § 90 b BGB vorgeschlagen: „Autonome Systeme sind keine Personen. Auf sie sind die für Hilfspersonen geltenden Vorschriften entsprechend anzuwenden, soweit nicht etwas anderes bestimmt ist.“⁵⁴ Dagegen sollen KI-Systeme über kein eigenes Vermögen verfügen, also auch nicht selbständig Träger von Rechten oder Pflichten sein.⁵⁵

[27] Gegen diese Aufspaltung der Rechtsfähigkeit sprechen jedoch bereits gravierende dogmatische Bedenken:⁵⁶ Eine Entität kann entweder Träger von Rechten und Pflichten sein oder nicht; eine Teilrechtsfähigkeit ist dabei nicht vorstellbar. Sobald eine Entität irgendein Recht haben kann, ist sie rechtsfähig.⁵⁷ Auf einem anderen Blatt steht die Selbstverständlichkeit, dass nicht jedes Rechtssubjekt die Voraussetzungen jeder Rechtsnorm erfüllen kann, sodass bestimmte Subjekte trotz ihrer Rechtsfähigkeit bestimmte Rechte nicht erwerben können. Die These von der „funktionell bestimmten Teilrechtsfähigkeit“ führt letztlich zu einem willkürlichen Rosinenpicken hinsichtlich der Voraussetzungen und Folgen von Rechtsfähigkeit,⁵⁸ dessen dogmatische Folgewirkungen nicht absehbar sind.

[28] Zudem kann die Lehre von der Teilrechtsfähigkeit ihr eigenes Ziel, das Schließen der „Verantwortungslücke“, nicht erreichen. Solange ihr Zweck nur darin besteht, die Zurechnungsregeln der §§ 164 ff., 278 BGB anwendbar zu machen, bleibt die Frage nach der lückenschließenden Eigenhaftung des Stellvertreters aus § 179 BGB ohne eigenes Vermögen ungelöst. Von vornherein auf diese Weise nicht lösbar ist die Haftungslücke im Deliktsrecht, weil das deutsche Recht hier – abgesehen von § 31 BGB – keine Regeln über die Zurechnung des Verhaltens Dritter kennt, sodass für alle Fälle der Exkulpation des Hintermannes eine Eigenhaftung der Hilfsperson erforderlich ist.⁵⁹ Stets ist die Eigenhaftung der Hilfsperson wesentlicher Teil des gesetzlichen Regelungssystems, die nicht über die willkürliche Konstruktion einer bloßen Teilrechtsfähigkeit ausgeschaltet werden darf.

[29] Im Recht der Stellvertretung sind daraus nur zwei Auswege denkbar: Entweder werden Einschränkungen der Vertretungsmacht für unwirksam erklärt,⁶⁰ dann handelt es sich aber nicht mehr um Stellvertretung, sondern faktisch um eine unmittelbare und unbeschränkte Zurechnung der Erklärungen des KI-Systems an den Betreiber.⁶¹ Oder die Haftung des KI-Systems nach § 179 BGB wird explizit ausgeschlossen, z. B. durch

Gleichstellung mit einem minderjährigen Stellvertreter (§ 179 III 2 BGB).⁶² Damit würde allerdings das Risiko einer Vollmachtüberschreitung dem Vertragspartner zugewiesen, ohne dass – anders als im originären Anwendungsbereich des § 179 III 2 BGB, dem Minderjährigenschutz⁶³ – überwiegende Schutzinteressen dies rechtfertigen würden.

[30] Lediglich für die vertragliche Schadensersatzhaftung würde die Einführung einer Teilrechtsfähigkeit die „Verantwortungslücke“ schließen, indem Fehlverhalten des KI-Systems dem Betreiber gem. § 278 BGB als eigenes Verhalten zugerechnet würde.⁶⁴ Freilich müsste auch nach dieser Auffassung jedenfalls das materielle Abgrenzungsproblem⁶⁵ gelöst werden, um diejenigen Systeme zu identifizieren, bei denen eine derartige unbedingte Zurechnung erfolgen soll. Wie bereits gezeigt, dürfte dies nicht rechtssicher möglich sein.

V. Ausblick: Alternativen zur Rechtsfähigkeit

[31] Weder die Zuerkennung vollständiger Rechtsfähigkeit noch die Lehre von der Teilrechtsfähigkeit sind mithin geeignet, die sogenannte „Verantwortungslücke“ zu schließen. Wie abschließend kurz zu skizzieren sein wird, sind diese Konstruktionen für ein angemessenes Zurechnungs- und Haftungsregime auch nicht erforderlich.

[32] Im Vertragsrecht sollten Erklärungen von KI-Systemen unmittelbar als eigene Erklärungen des Betreibers angesehen werden, ohne dass die Regeln des Stellvertretungsrechts zur Anwendung gelangen (Lehre von der Computererklärung).⁶⁶ Der Einsatz des Systems und

⁵³ Die Begriffe variieren: Von „teilrechtsfähigen Subjekten“ sprechen *Schirmer* JZ 2016, 660 (663 ff.); *ders.* JZ 2019, 711 ff.; *Specht/Herold* MMR 2018, 40 (43); *Herold*, Vertragsschlüsse unter Einbeziehung automatisiert und autonom agierender Systeme, 2020, 195 ff.; von „partieller Rechtssubjektivität“ *Teubner* AcP 218 (2018), 155 ff.; von „Teilrechtssubjekten“ *Beck/Gruber*, Jenseits von Mensch und Maschine, 133 ff.

⁵⁴ *Schirmer* JZ 2019, 711 (717).

⁵⁵ Ausdrücklich *Teubner* AcP 218 (2018), 155 (161 f.); *Schirmer* JZ 2016, 660 (665 f.); für die Zuerkennung von Vermögensfähigkeit nur „bei Bedarf“ auch *Beck/Gruber*, Jenseits von Mensch und Maschine, 133 (156).

⁵⁶ S. dazu auch *Klingbeil* JZ 2019, 718 (722); *Riehm/Meier* in DGRI Jahrbuch 2018, 1 (32 f.).

⁵⁷ *Lehmann* AcP 207 (2007), 225 (238).

⁵⁸ S. etwa die Überlegungen bei *Herold*, Vertragsschlüsse unter Einbeziehung automatisiert und autonom agierender Systeme, 211 ff.

⁵⁹ Allerdings möchte *Schirmer* JZ 2016, 660 (665) die Eigenhaftung von Robotern nicht an deren fehlender Vermögensfähigkeit scheitern lassen.

⁶⁰ In diese Richtung *Schirmer* JZ 2016, 660 (664).

⁶¹ Ebenso *Foerster* ZfPW 2019, 418 (426).

⁶² So ausdrücklich *Herold*, Vertragsschlüsse unter Einbeziehung automatisiert und autonom agierender Systeme, 215 ff.

⁶³ S. bereits *Riehm/Meier* in DGRI Jahrbuch 2018, 1 (33 f.).

⁶⁴ Darauf stellen *Schirmer* JZ 2019, 711 ff.; *Teubner* AcP 218 (2018), 155 ff. vorrangig ab.

⁶⁵ Oben III.2.b).

⁶⁶ So auch *Gitter*, Softwareagenten im elektronischen Geschäftsverkehr, 181 f.; *Auer*, Rechtsfähige Softwareagenten: Ein erfrischender Anachronismus, 30.9.2019, abrufbar unter: <https://beck-link.de/bna54>.

seine Konfiguration gehen ebenso wie seine Eigenschaft als selbstlernendes System auf den Willen seines Betreibers zurück. Dadurch hat er selbst das Risiko gesetzt, dass dieses System Erklärungen abgibt, die er nicht vorhergesehen hat (und profitiert zugleich von den damit verbundenen Chancen), was seine Bindung an diese Erklärungen rechtfertigt.⁶⁷ Das würde selbst dann gelten, wenn ein Betreiber ein Warenwirtschaftssystem mit einem Zufallsgenerator bei der Preisgestaltung versehen würde – warum sollte es für unvorhersehbare KI-Systeme anders sein?⁶⁸ Die risikobasierte Zurechnung von Willenserklärungen ist dem geltenden Recht ohnehin nicht fremd; die alleinige Anknüpfung an den tatsächlichen Willen des Erklärenden ist eine rechtliche Fiktion.⁶⁹ In der Folge hätte der Betreiber zugleich hinreichende Anreize, das System so zu konfigurieren und zu überwachen, dass es keine unvorhergesehenen Erklärungen abgibt. Nur ganz ausnahmsweise dürfte eine Irrtumsanfechtung analog § 120 BGB in Betracht kommen.⁷⁰

[33] Auch im Bereich der vertraglichen Schadensersatzhaftung ist eine weitgehend unbeschränkte Zurechnung des Verhaltens von KI-Systemen an ihren Betreiber *de lege lata* möglich. Ob hierzu § 278 BGB analog angewendet⁷¹ oder dem Betreiber eine entsprechende Garantieübernahme i. S. v. § 276 I a. E. BGB unterstellt wird,⁷² dürfte zweitrangig sein; die §§ 276 ff. BGB sind jedenfalls hinreichend flexibel, um den Schuldner für die Handlungen der von ihm eingesetzten Computersysteme unabhängig von deren Autonomiegrad einstehen zu lassen.⁷³ Hierin liegt jedenfalls ein wesentlich geringfügigerer Eingriff in die dogmatischen Grundlagen des Zivilrechts als in der Schaffung einer Teilrechtsfähigkeit.

[34] Im Deliktsrecht sorgen zunächst die Gefährdungshaftungstatbestände für die Halter von Kraft-, Schienen- und Luftfahrzeugen (§§ 7 StVG, 1 HaftPflG, § 33 LuftVG) für eine nahezu unbeschränkte Haftung des Betreibers entsprechender autonomer Fahrzeuge.⁷⁴ Für andere autonome Systeme dürfte die Haftungsfrage zunächst mit einer einzelfallbezogenen Definition und ggfs. Erweiterung der Verkehrspflichten im Umgang mit KI-Systemen befriedigend gelöst werden. Zusätzlich kommt eine Übertragung der Beweislastverteilung aus § 831 I BGB in Betracht, sodass Betreiber sich exkulpieren müssen, wenn ihre KI-Systeme Rechtsgutsverletzungen verursachen.⁷⁵ Eine Anerken-

nung von Teilrechtsfähigkeit ist auch hier nicht erforderlich, wie sich an § 833 BGB zeigt, der dieselbe dogmatische Konstruktion im Hinblick auf – zweifellos nicht rechtsfähige – Nutztiere vorsieht. Erst wenn sich auch dann noch Haftungslücken zeigen sollten, könnte *de lege ferenda* an die Entwicklung eines Gefährdungshaftungstatbestandes zulasten der Betreiber gedacht werden.⁷⁶

[35] Keinesfalls sollte die Zuerkennung von Rechtsfähigkeit an KI-Systeme dazu genutzt werden, Hersteller und Betreiber weitgehend aus ihrer Verantwortung für das „Verhalten“ ihrer Systeme zu entlassen. Denn dadurch würde für sie ein wesentlicher Anreiz entfallen, sichere Systeme zu schaffen bzw. im laufenden Betrieb für deren Sicherheit zu sorgen.⁷⁷ Durch die unbeschränkte Zurechnung des Verhaltens von KI-Systemen treffen Chancen und Risiken des Einsatzes dieser Systeme dagegen stets den Betreiber, sodass er bei der Auswahl und Konfiguration ebenso wie bei der Entscheidung über das Ob und den Umfang des Einsatzes von KI-Systemen sämtliche Haftungsrisiken mit berücksichtigen kann und wird.

⁶⁷ Ebenso Foerster ZfPW 2019, 418 (427).

⁶⁸ S. auch die Parallele zur Zurechnung von Blanketterklärungen bei Grapentin, Vertragsschluss und vertragliches Verschulden beim Einsatz von künstlicher Intelligenz und Softwareagenten, 100; Schulz, Verantwortlichkeit bei autonom agierenden Systemen, 127 f.

⁶⁹ Eingehend hierzu Rebbert, Das Rechtfertigungsprinzip, 2014.

⁷⁰ So – allerdings im Kontext eines deterministischen Warenwirtschaftssystems – BGH NJW 2005, 976.

⁷¹ In diese Richtung Datenethikkommission, Gutachten, 219 (8.2.2); Hilgendorf/Hanisch, Robotik im Kontext von Recht und Moral, 27 (59 f.); Zech ZfPW 2019, 198 (211); abl. Grapentin, Vertragsschluss und vertragliches Verschulden beim Einsatz von künstlicher Intelligenz und Softwareagenten, 131; Schulz, Verantwortlichkeit bei autonom agierenden Systemen, 138 ff.

⁷² Angedacht bei Klingbeil JZ 2019, 718 (722 f.); Schulz, Verantwortlichkeit bei autonom agierenden Systemen, 141.

⁷³ Für eine Darstellung möglicher Sorgfaltspflichten s. Grapentin, Vertragsschluss und vertragliches Verschulden beim Einsatz von künstlicher Intelligenz und Softwareagenten, 132 ff.

⁷⁴ S. nur Zech ZfPW 2019, 198 (214 f.).

⁷⁵ Ähnlich Hilgendorf/Hanisch, Robotik im Kontext von Recht und Moral, 27 (59 f.); Zech ZfPW 2019, 198 (211); zurückhaltend allerdings Schulz, Verantwortlichkeit bei autonom agierenden Systemen, 146 ff.; s. auch Foerster ZfPW 2019, 418 (433): Sekundäre Darlegungslast des Halters.

⁷⁶ In diese Richtung auch Spindler JZ 2016, 805 (816); Lohmann ZRP 2017, 168 (171); Seelmann/Gless/Janal, Intelligente Agenten und das Recht, 141 (155 ff.); konkreter Gesetzgebungsvorschlag hierzu bei Hilgendorf/Hanisch, Robotik im Kontext von Recht und Moral, 27 (54); für Gefährdungshaftung des Herstellers Eidenmüller ZEuP 2017, 765 (772).

⁷⁷ Lohsse/Schulze/Staudenmayer/Wagner, Liability for Artificial Intelligence and the Internet of Things, 27 (57); Hilgendorf/Hanisch, Robotik im Kontext von Recht und Moral, 27 (39 f.).

E-JUSTICE/E-GOVERNMENT

PD Dr. Martin Fries/Prof. Dr. Rupprecht Podszun/RiLG Benedikt Windau*

Virtuelle Verhandlung statt fliegendem Gerichtsstand

Fairer Wettbewerb durch technischen Fortschritt

Die Einschränkung des „fliegenden Gerichtsstands“ für UWG-Verfahren hat für viel Aufsehen gesorgt. Einige lauterkeitsrechtliche Verfahren, die bislang nach dem Tatortprinzip quasi überall in Deutschland geführt werden konnten, müssen nun am Sitz des Beklagten angestrengt werden. Beide Modelle – Klage am Ort der Rechtsverletzung einerseits und Klage am Sitz des Beklagten andererseits – haben jeweils Vor- und Nachteile. Die Autoren plädieren dafür, am „fliegenden Gerichtsstand“ festzuhalten und dabei die Möglichkeiten einer virtuellen Teilnahme auszuweiten. UWG-Fälle sind dafür besonders geeignet. Sie könnten damit auch zum Test für die Ausweitung einer Online-Gerichtsbarkeit in andere Rechtsbereiche werden.

I. Der Gerichtsstand in Wettbewerbsprozessen

[1] Der Gerichtsstand im Lauterkeitsrecht ist ein Politikum. Bei der jüngsten Reform des Gesetzes gegen den unlauteren Wettbewerb (UWG) durch das Gesetz zur Stärkung des fairen Wettbewerbs¹ wurde energisch darüber gestritten, welches Gericht für UWG-Verletzungen zuständig sein soll.²

1. Neuregelung durch das Gesetz zur Stärkung des fairen Wettbewerbs

[2] Typischerweise sind UWG-Streitigkeiten von Unterlassungsansprüchen nach § 8 I UWG geprägt, die mit Abmahnungen, einstweiligen Verfügungen und gelegentlich auch im Hauptsacheverfahren durchgesetzt werden. Hierfür war bisher nach § 14 II 1 UWG das Gericht am Begehungsort zuständig. Dieser Begriff wiederum umfasste nicht nur den Handlungs-, sondern gerade auch den Erfolgsort,³ was insbesondere in Mediensachen dazu führte, dass Mitbewerber bundesweit eine völlig freie Gerichtsstandswahl genossen. Freilich hatte die Rechtspraxis das dadurch mögliche *forum shopping* immer wieder eingegrenzt. So wurde beispielsweise verlangt, dass die Verbreitung „bestimmungsgemäß“ in einem Gebiet erfolgte.⁴ Ein Blick in die Entstehungsgeschichte der Vorschrift zeigt, dass der Gesetzgeber seit 1909 mehrfach bei der örtlichen Zuständigkeit nachjustiert hat.⁵

[3] Diesen Weg wollte der Gesetzgeber mit der Neuregelung 2020 fortsetzen und dabei dem Vorbild des Urheberrechts folgen, wo beim Vorgehen gegen natürliche Personen (!) der fliegende Gerichtsstand 2013 unter bestimmten Voraussetzungen – vgl. § 104 a I UrhG – aufgehoben wurde.⁶ Der im legislativen Verfahren mehrfach neugefasste § 14 II UWG sieht nunmehr vor, dass grundsätzlich Ansprüche dort geltend zu machen sind, wo der Beklagte seinen allgemeinen Gerichtsstand hat. Der Ort der Zuwiderhandlung kann nur für Unterlassungsansprüche von Mitbewerbern genutzt werden, soweit es nicht um „Rechtsstreitigkeiten wegen Zuwiderhandlungen im elektronischen Ge-

* Der Autor Fries ist Privatdozent an der Juristischen Fakultät der Ludwig-Maximilians-Universität München. Der Autor Podszun ist Inhaber des Lehrstuhls für Bürgerliches Recht, deutsches und europäisches Wettbewerbsrecht an der Heinrich-Heine-Universität Düsseldorf. Der Autor Windau ist Richter am Landgericht Oldenburg. Sämtliche Internetquellen wurden zuletzt am 27.10.2020 abgerufen.

1 Zum Zeitpunkt des Redaktionsschlusses dieses Beitrags war das Gesetz verabschiedet, aber noch nicht veröffentlicht. Der letzte Stand des hier relevanten § 14 II 2 UWG-E findet sich in BT-Drucks. 19/22238, S. 8.

2 Zur Diskussion u. a. *Lerach* GRUR-Prax 2020, 37; *Möller* ZRP 2018, 200 (203); *Löffel* NJW-Editorial Heft Nr. 40/2020; *Fritzsche* WRP 2020, 1367, sowie die Stellungnahmen zum Gesetzentwurf, abrufbar unter: <https://beck-link.de/87cez>.

3 *Ohly/Sosnitzer/Sosnitzer*, UWG, 7. Aufl. 2016, § 14 Rn. 10 f.; *Teplitzky/Schaub*, Wettbewerbsrechtliche Ansprüche und Verfahren, 12. Aufl. 2019, Kap. 45 Rn. 13.

4 *OLG Karlsruhe* WRP 1976, 490.

5 Siehe *Harte-Bavendamm/Henning-Bodewig/Retzer/Tolkmitt*, UWG, 4. Aufl. 2016, § 14 Rn. 1 ff.

6 Vgl. *Schulte-Nölke/Henning-Bodewig/Podszun*, Evaluation der Verbraucherschützenden Regelungen im Gesetz gegen unseriöse Geschäftspraktiken, 2017, S. 239.

schäftsverkehr oder in Telemedien“ geht.⁷ Ziel dieser Novellierung ist die Eindämmung von „Abmahnmissbrauch“:⁸ Der Gesetzgeber möchte verhindern, dass Abmahnungen vorrangig zur Erzielung von Gebühren und Vertragsstrafen ausgesprochen werden.⁹ Insbesondere kleine und mittlere Unternehmen sollen davor geschützt werden, dass einstweilige Verfügungen gezielt bei von ihrem Sitz weit entfernten Gerichten beantragt werden, um ihnen die Rechtsverteidigung zu erschweren.¹⁰ Zudem soll verhindert werden, dass Antragsteller/Kläger gezielt Gerichte auswählen, die ihre Rechtsauffassung mutmaßlich teilen, zügig einstweilige Verfügungen erlassen oder Streitwerte großzügig bestimmen.¹¹

2. Diskussionsprozess

[4] Für eine Abschaffung des fliegenden Gerichtsstands hatten sich in der rechtspolitischen Diskussion vor allem einige Unternehmensverbände stark gemacht. Politischen Auftrieb erhielt das Argument im Zuge der Debatte über die DSGVO und eine zeitweilig erwartete „Abmahnwelle“ im Datenschutzrecht.¹² Man befürchtete, kleine Unternehmen könnten wegen Bagatellverstößen beim Webseitenbetrieb mit kostspieligen Abmahnungen überzogen werden, gegen die sie sich nur bei weit entfernten, klägerfreundlichen Gerichten würden wehren können.¹³ Die zuweilen emotional geführte Diskussion wirft die Frage auf, was eigentlich die wesentlichen Parameter zur Bestimmung der Sinnhaftigkeit eines Gerichtsstands sind. Wo sollte nach der gesetzgeberischen Vorstellung geklagt werden, wenn es keine gültige Vereinbarung der Parteien dazu gibt?

[5] Ausgangspunkt für solche Überlegungen sind das Recht auf den gesetzlichen Richter und die prozessuale Waffengleichheit sowie im vorliegenden Fall Art. 7 VO (EU) Nr. 1215/2012. Zunächst gilt die Überlegung, dass derjenige, der als Beklagter zur Einlassung gezwungen wird, wenigstens das Privileg genießen sollte, an seinem Ort verklagt zu werden. Bei diesem Gerechtigkeitsgrundsatz bleibt der Gesetzgeber aber nicht stehen. Hinzu treten Zweckmäßigkeitserwägungen, die im Ergebnis zu einem ausdifferenzierten gesetzlichen System der Zuständigkeitszuweisung geführt haben.¹⁴

[6] Für die Abschaffung des fliegenden Gerichtsstands wird traditionell angeführt, Gerichte benötigten regelmäßig besondere Kenntnisse über den Ort des Beklagensitzes und lokale Handelsbräuche, Zeugen hätten ohne fliegenden Gerichtsstand eine einfachere Anreise, und der Beklagte tue sich leichter mit der Wahl eines Anwalts an seinem Sitz.¹⁵ Kritiker der Gesetzgebungsinitiative verwiesen demgegenüber darauf, der Gerichtsstand am Erfolgsort entspreche einer – auch in § 32

ZPO niedergelegten – allgemeinen Wertentscheidung des Gesetzgebers, ein Vergleich mit dem Urheberrecht passe nicht, weil es bei der dortigen Rechtsänderung nur um Rechtsverletzungen Privater gegangen sei, und zudem stehe eine Verletzung von Art. 7 Nr. 2 VO (EU) Nr. 1215(2012) wegen Ausländerdiskriminierung im Raum. Vor allem aber ermögliche nur der fliegende Gerichtsstand die notwendige große Sachkunde der befassten Gerichte im Umgang mit UWG-Streitigkeiten,¹⁶ und ohnehin mangle es an einer empirischen Basis für die Behauptung, es gebe im großen Stil missbräuchliche Abmahnungen.¹⁷

3. Parameter einer Lösung

[7] Versucht man, diese engagiert geführte Debatte für eine sinnvolle Neuregelung fruchtbar zu machen, lässt sich eine Reihe von Erkenntnissen ableiten. Zunächst: Entfernt liegende Gerichte treiben die Kosten für eine Seite in die Höhe und machen die Rechtsverteidigung schwierig. Hier gibt es durchaus ein gewisses Missbrauchspotenzial.¹⁸ Entfernungskosten sollten insofern tunlichst vermieden werden.

[8] Zugleich ist eine aus einer Vielzahl von Fällen gewonnene Expertise bei einzelnen Gerichten wünschenswert, auch als Standortfaktor. Die große Anerkennung, die man den besonders häufig angerufenen Landgerichten allenthalben zollt, ist auf ihre ständige Befassung mit der Materie und die dadurch ausgebildete besondere UWG-Kenntnis zurückzuführen. Die GRUR hat nach

⁷ BT-Drs. 19/22238, S. 8.

⁸ BT-Drs. 19/12084, S. 1. Freilich steht der fliegende Gerichtsstand mit Abmahnungen nur mittelbar in Zusammenhang, als Drohung für den nachfolgenden Antrag auf Erlass einer einstweiligen Verfügung oder die Klageerhebung.

⁹ BT-Drs. 19/12084, S. 1.

¹⁰ BT-Drs. 19/12084, S. 20.

¹¹ BT-Drs. 19/12084, S. 35.

¹² Vgl. Deutscher Bundestag, Wissenschaftliche Dienste: Abmahnungen im Datenschutzrecht, 2018, WD7-3000-116/18, S. 4.

¹³ Ein weiterer Hebel speziell zur Vermeidung solcher Abmahnungen ist in § 13 IV UWG n. F. durch einen Ausschluss des Aufwendungsersatzanspruchs vorgesehen.

¹⁴ Musielak/Voit/Heinrich, ZPO, 17. Aufl. 2020, § 12 Rn. 1; Stein/Jonas/Roth, ZPO, 23. Aufl. 2014, Vor § 12 Rn. 3; MüKoZPO/Patzina, 6. Aufl. 2020, § 12 Rn. 2.

¹⁵ BT-Drs. 19/12084, S. 35 f.; DIHK, Stellungnahme vom 28.9.2018, S. 12, abrufbar unter: <https://beck-link.de/482e8>; ZDH, Stellungnahme vom Oktober 2018, abrufbar unter: <https://beck-link.de/6r2cx>.

¹⁶ Ahrens in FS Harte-Bavendamm, 2020, S. 453, 460; Max-Planck-Institut für Innovation und Wettbewerb, Stellungnahme vom 11.9.2018, abrufbar unter: <https://beck-link.de/6r2cx>; Vereinigung für gewerblichen Rechtsschutz und Urheberrecht e.V. (GRUR), Stellungnahme vom 15.10.2018, abrufbar unter: <https://beck-link.de/23zrf>; BDI, Stellungnahme vom 4.10.2018, abrufbar unter: <https://beck-link.de/v43s2>; Pres/Voßberg, zpoblog v. 14.9.2020, abrufbar unter: <https://www.zpoblog.de/?p=8781>. Dem Spezialisierungsargument wurde entgegengehalten, eine Spezialisierung sei im UWG verzichtbar, zudem schaffe § 14 III UWG weitgehende Konzentrationsmöglichkeiten für die Landesjustizverwaltungen; BT-Drs. 19/12084, S. 36.

¹⁷ DAV, Stellungnahme Nr. 48/2018, S. 11, abrufbar unter: <https://beck-link.de/fy834>. Vgl. auch den Vortrag von Loschelder, Zur geplanten Evaluierung des fliegenden Gerichtsstands im UWG, o. D., Folien 13 ff., abrufbar unter: <https://beck-link.de/cr7de>.

¹⁸ Vgl. LG Aurich MMR 2013, 249.

Auswertung veröffentlichter Entscheidungen festgestellt, dass es im Wesentlichen sieben Gerichte sind, die die UWG-Rechtsprechung in Deutschland prägen: Hamburg, München I, Düsseldorf, Köln, Berlin, Frankfurt am Main und Stuttgart.¹⁹ Deren Stellung als Kompetenzzentren würde durch die Aufwertung des Sitzes nivelliert. Eine Neuregelung sollte insofern möglichst dazu führen, dass es zu einer Konzentration der Fälle bei einzelnen Gerichten kommt.

[9] Ein salomonischer Fingerzeig zur Auflösung dieses Dilemmas könnte sich nun aus den Erfahrungen der Justiz in Zeiten der COVID-19-Pandemie ergeben. Die Rechtspflege hat in dieser Zeit gelernt, dass die Verhandlung im Wege der Bild- und Tonübertragung nach § 128 a ZPO kein reiner Notnagel ist, sondern bei entsprechender Ausstattung der Gerichte in vielen Fällen eine echte Alternative zur klassischen Präsenzverhandlung darstellt. Es liegt nahe, die Möglichkeit solcher Videokonferenzverhandlungen in UWG-Streitigkeiten systematisch zu nutzen, um die jahrzehntelang aufgebaute Spezialisierung einzelner Landgerichte in diesem Bereich nicht zu verspielen und zugleich unvorteilhafte Klageanreize zu vermeiden.²⁰ Es wird immer einzelne Verfahren geben, für die eine Verhandlung nach § 128 a ZPO nicht so gut geeignet sein mag wie eine klassische Gerichtsverhandlung. Für die Gestaltung des Verfahrensrechts sollten aber nicht kleine Nachteile in außergewöhnlichen Ausreißer-Fällen maßgeblich sein, sondern der große Vorteil für die breite Mehrheit aller Verfahren.

II. Eignung des UWG-Verfahrens für eine „Virtualisierung“

[10] Warum eignen sich gerade UWG-Verfahren in besonderem Maße für eine Ausweitung der Möglichkeiten virtueller Verhandlungen? Im UWG-Verfahren sind die Landgerichte ausschließlich zuständig (§ 14 I UWG). Die Amtsgerichte mit ihren spezifischen Anforderungen sind gar nicht erst betroffen. Darüber hinaus ist das UWG-Verfahren von professionellen Akteuren auf beiden Seiten, von geringen Beweisanforderungen und von einem hohen Tempo gekennzeichnet – alles Aspekte, die solche Verfahren für eine Video-Übertragung als ideal geeignet erscheinen lassen.

1. Beteiligte

[11] Im UWG-Verfahren stehen sich immer professionelle Anspruchsberechtigte und Anspruchspflichtige gegenüber: Aktivlegitimiert ist lediglich der in § 8 III UWG genannte Personenkreis, insbesondere Mitbewerber und Verbände. Schuldner des UWG-Anspruchs sind in der Praxis in aller Regel Unternehmen. Zudem sind Personen ohne eigene Entscheidungsspielräume wie der klassische Prospektverteiler von der Haftung ausgenom-

men.²¹ Unternehmen und Verbände sind IT-affin und verfügen in der Regel über eine funktionstüchtige Computerausstattung. Besondere technische Voraussetzungen sind für die Verhandlung heute kaum mehr erforderlich, weil eine Teilnahme im Wege der Bild- und Tonübertragung technisch meistens schon über einen Browser zusammen mit einem Laptop, Tablet oder Smartphone möglich ist.²²

2. Beweisaufnahmen

[12] Gelegentlich wird gegen Verfahren nach § 128 a ZPO eingewandt, diese eigneten sich nicht für wichtige Beweisaufnahmen.²³ UWG-Verfahren sind jedoch häufig durch Rechtsfragen gekennzeichnet, komplexe Beweisaufnahmen sind selten.²⁴ In aller Regel werden Verfahren nach eigener Sachkunde des Gerichts entschieden, dies gilt insbesondere für den meist strittigen und oft entscheidungserheblichen Punkt der Verkehrsauffassung.²⁵ UWG-Verfahren lassen sich deshalb überdurchschnittlich gut allein im schriftlichen Verfahren durchführen.

[13] Geht es um „Schriftstücke“ wie z. B. eine Anzeige in einer Zeitschrift, einen Werbeflyer, ein Angebot im Internet oder Fotos von einer Ladenaufmachung, wird deren Gestaltung in der Regel unstrittig sein, so dass ein Augenscheinsbeweis im engeren Sinne entbehrlich ist. Ähnliches gilt, wenn die unlautere Nachahmung (§ 4 Nr. 3 UWG) eines Produkts in Rede steht. Selbst wenn das Gericht z. B. wegen der Einzelheiten einer dreidimensionalen Gestaltung eines Produkts eine Augenscheinseinnahme im Gerichtssaal gem. § 371 ZPO für erforderlich hält, steht dies einer Teilnahme der Parteien bzw. ihrer Bevollmächtigten im Wege der Bild- und Tonübertragung nicht entgegen, denn das Gericht kann einen vorab übersandten Gegenstand auch im Gerichtssaal gem. § 371 ZPO in Augenschein nehmen, wenn die Parteien sich an einem anderen Ort aufhalten.²⁶ Auf die

¹⁹ GRUR (Fn. 16), S. 5.

²⁰ Die anfallenden Kosten sind dabei absolut überschaubar: Es fällt lediglich gem. Ziff. 9019 KV-GKG eine Gebühr von 15 Euro je angefangener halben Stunde an, die angesichts der Streitwerte und Gerichtskosten in UWG-Sachen nicht wirklich ins Gewicht fallen wird. S. dazu auch ausführlich Windau, Kostenrechtliche Fragen der Verhandlungen im Wege der Bild- und Tonübertragung, abrufbar unter: <https://www.zpoblog.de/?p=8673>.

²¹ Ahrens/Jestaedt, Der Wettbewerbsprozess, 8. Aufl. 2017, Kap. 21 Rn. 19 f.

²² Dazu Mantz/Spoenle MDR 2020, 637 Rn. 18; s. zu den von den Bundesländern verwendeten Systemen auch <https://www.zpoblog.de/service/128a-technik-bundeslaender/>.

²³ Sehr instruktiv Greger MDR 2020, 957 (960); ähnlich Schmidt/Saam ZRP 2020, 216 (218); tendenziell auch Mantz/Spoenle MDR 2020, 637 Rn. 25.

²⁴ Treffend Teplitzky/Schwippert, Wettbewerbsrechtliche Ansprüche und Verfahren, Kap. 47 Rn. 3: „Der im allgemeinen Prozessrecht mehr theoretische Grundsatz, dass nicht jede streitige rechtserhebliche Tatsache – auch soweit sie nicht offenkundig oder i. S. der §§ 291 f. ZPO zu vermuten ist – des Beweises bedarf, hat im Wettbewerbs- und Markenrecht erhebliche praktische Bedeutung gewonnen.“

²⁵ Vgl. Ahrens/Bähr, Der Wettbewerbsprozess, Kap. 27 Rn. 4 ff.

²⁶ Ebenso Gehrlein ZMR 2020, 257 (263).

äußerst umstrittenen Frage, ob § 128 a ZPO auch einen „Teleaugenschein“ (ohne Zustimmung der Parteien, vgl. § 284 S. 2 ZPO) zulässt,²⁷ wird es kaum ankommen, weil es – soweit erkennbar – keine Ortstermine in UWG-Sachen gibt. Und soweit es einmal um die Anhörung eines Zeugen geht, der als „präsenzer Zeuge“ gehört werden soll, handelt es sich bei solchen Personen in der Regel auch um Personen, die im wirtschaftlichen Verkehr tätig sind. Für ihre Beteiligung in einem für sie fremden Rechtsstreit wäre der Aufwand einer Reise zu einem entfernten Gericht allemal höher als die Teilnahme per Video.

3. Rechtliches Gehör und Waffengleichheit

[14] In UWG-Verfahren ist die Anhörung beider Seiten nach den BVerfG-Entscheidungen zu dieser Thematik²⁸ erst recht ein wichtiger Punkt. Schutzschriften spielen dafür eine Rolle, aber auch sonstige Möglichkeiten der Kontaktaufnahme. In einem weitgehend online geführten Verfahren liegt es daher nahe, das rechtliche Gehör nicht nur durch einen Telefonanruf zu gewähren, weil dies eine faire Einbeziehung ins Verfahren schwierig macht. Je nach Ausgestaltung des Verfahrens und personeller Ausstattung könnte das Gericht sogar binnen weniger Stunden oder am Folgetag eine vollwertige – virtuelle – mündliche Verhandlung durchführen.

4. Geschwindigkeit

[15] Kennzeichen der UWG-Verfahren ist vor allem die Geschwindigkeit, mit der sie abgewickelt werden. Dabei ist natürlich ausschlaggebend, dass ein Großteil der Verfahren auf Unterlassungsstreitigkeiten im einstweiligen Rechtsschutz entfällt. Die Beteiligten haben nach dem Eilrechtsschutz häufig kein Bedürfnis mehr für ein Hauptsacheverfahren. Schadensersatzfälle und vor allem Ansprüche auf Gewinnabschöpfung sind außerordentlich selten. Gerade die Dominanz der Unterlassungsansprüche im einstweiligen Rechtsschutz spricht dafür, ein möglichst rasches Verfahren mit geringen Hürden vorzusehen.

[16] Ein Spezialthema des UWG (wie des Immaterialgüterrechts) können Messen sein, auf denen es zu Rechtsverstößen kommt, etwa weil Produkte in unlauterer Weise angepriesen werden. Gerade diese Fälle sind insofern UWG-typisch, als die Schnelligkeit des Verfahrens eine überragende Rolle spielt. Diese Schnelligkeit ließe sich mit einem ortsunabhängigen reinen Online-Gericht sogar noch leichter schaffen als durch ein ortsansässiges Gericht, selbst wenn dieses in derselben Stadt residieren sollte wie der Messestandort. Die Antragstellerin könnte vom Messegelände aus das Online-Verfahren starten. Müsste sie erst im Berufsverkehr von der Messe zu Gericht fahren, um ihren Antrag zu stellen, könnte wertvolle Zeit verstreichen.

III. Ausweitung bestehender Möglichkeiten

[17] Wie lässt sich die vermehrte Nutzung virtueller Gerichtsverhandlungen innerhalb des bestehenden Regelungsrahmens umsetzen? Grundlage hierfür wäre das Konzept des seit 20 Jahren geltenden § 128 a ZPO²⁹. Diese Vorschrift ermöglicht es dem Gericht schon heute, sämtlichen Beteiligten zu gestatten, sich während der Verhandlung bzw. Vernehmung außerhalb des Gerichtssaals aufzuhalten; lediglich das Gericht muss dort präsent sein. § 128 a ZPO ermöglicht insofern keine besondere Form der (Online-)Verhandlung, sondern lediglich eine besondere Form der Teilnahme an einer Verhandlung.

[18] Die praktische Bedeutung dieser Vorschrift ist allerdings bisher gering, weil es einerseits auf anwaltlicher und gerichtlicher Seite Vorbehalte gibt und weil es andererseits in den meisten Gerichtssälen an der dafür erforderlichen Technik fehlt. Deswegen werden dahingehende Anträge unter Berufung auf die fehlende technische Ausstattung regelmäßig zurückgewiesen.³⁰

[19] Für die Regelung in § 128 a I und II ZPO sind dabei zwei Parameter bedeutsam: Es steht im pflichtgemäßen³¹ Ermessen des Gerichts, ob es den Parteien und ihren Bevollmächtigten während der Verhandlung (I) bzw. Zeugen oder Sachverständigen während der Vernehmung (II) gestattet, im Wege der Bild und Tonübertragung teilzunehmen. Und die Teilnahme im Wege der Bild- und Tonübertragung ist immer freiwillig; auch bei einer Gestattung bleibt es den Beteiligten unbenommen, im Gerichtssaal körperlich anwesend an der Verhandlung teilzunehmen. Um eine möglichst große Akzeptanz einer Sonderregelung im UWG zu gewährleisten, spricht *a priori* einiges dafür, das Prinzip der Freiwilligkeit zunächst beizubehalten, aber an der „Stellschraube“ des gerichtlichen Ermessens zu „drehen“ und auf diese Weise möglicherweise auch darauf hinzuwirken, dass die technische Ausstattung der Gerichte zeitnah verbessert wird.

1. Teilnahme im Wege der Bild- und Tonübertragung als „Soll-Vorschrift“

[20] Diesen Weg hat der Gesetzgeber bereits in der Arbeits- und Sozialgerichtsbarkeit beschritten: Dort hat

²⁷ Bejahend BeckOK-ZPO/von Selle, 38. Edition, 1.9.2020, § 128 a Rn. 10; Zöller/Greger, ZPO, 33. Aufl. 2020, § 128 a Rn. 3; Schultzky NJW 2003, 313 (316); a. A. Musielak/Voit/Stadler, § 128 a Rn. 5.

²⁸ BVerfG WRP 2017, 1073; WRP 2018, 1443 und 1448; dazu Mantz NJW 2020, 2007; Löffel WRP 2019, 8.

²⁹ Für Dolmetscher*innen trifft § 185 I a GVG eine entsprechende Regelung.

³⁰ S. instruktiv ArbG Düsseldorf BeckRS 2020, 17871.

³¹ MüKoZPO/Fritsche, § 128 a Rn 7; es spricht allerdings viel für eine Ermessensreduktion aufgrund der gegenwärtigen Corona-Pandemie, s. nur Mantz/Spoenle MDR 2020, 637 Rn. 28.

er zu Beginn des Jahres³² das Ermessen aus Gründen des Gesundheitsschutzes im Fall einer epidemischen Lage von nationaler Tragweite i. S. d. § 5 I InfSG deutlich eingeschränkt, §§ 114 III ArbGG, 211 III SGG.³³ Das Gericht *soll* nun den Beteiligten in einem solchen Fall eine Teilnahme im Wege der Bild- und Tonübertragung gestatten. Dem folgend könnte der Gesetzgeber im UWG ebenfalls bestimmen, dass das Gericht den Beteiligten – unabhängig von einer epidemischen Lage – eine Teilnahme im Wege der Bild- und Tonübertragung gestatten *soll*.³⁴ § 14 II 4 UWG könnte dann wie folgt lauten:

„Für alle bürgerlichen Rechtsstreitigkeiten, mit denen ein Anspruch auf Grund dieses Gesetzes geltend gemacht wird, ist das Gericht zuständig, in dessen Bezirk der Beklagte seinen allgemeinen Gerichtsstand hat. Für alle bürgerlichen Rechtsstreitigkeiten, mit denen ein Anspruch auf Grund dieses Gesetzes geltend gemacht wird, ist außerdem das Gericht zuständig, in dessen Bezirk die Zuwiderhandlung begangen wurde.“

Das Gericht soll den Beteiligten gestatten, an Verhandlungen und Vernehmungen des Gerichts im Wege der Bild- und Tonübertragung (§ 128 a ZPO) teilzunehmen.“

[21] Üben die Gerichte ihr Ermessen entsprechend dieser Soll-Vorschrift aus, könnten dann regelmäßig sämtliche Beteiligte im Wege der Bild- und Tonübertragung teilnehmen. Das vom Gesetzgeber aufgeworfene Problem der durch Reiseaufwand verursachten Verhaltensfehlansätze wäre damit weitgehend gelöst.

2. Teilnahme im Wege der Bild- und Tonübertragung immer zulässig

[22] Eine solche, „weiche“ Regelung hätte freilich eine Schwäche: In der praktischen Umsetzung von §§ 114 III ArbGG, 211 III SGG hat sich gezeigt, dass die Länder vielfach gar nicht daran denken, die Arbeits- und Sozialgerichte mit der notwendigen Technik auszustatten, um eine Umsetzung der §§ 114 III ArbGG, 211 III SGG zu ermöglichen.³⁵ Anträge werden deshalb nach wie vor mit der Begründung zurückgewiesen, dass es an der notwendigen Technik fehle.³⁶ Die neu geschaffenen Regelungen laufen daher jedenfalls teilweise leer.

[23] Um den erforderlichen Paradigmenwechsel zu erzwingen, erscheint es daher deutlich sinnvoller, dass der Gesetzgeber die Entscheidung über die Möglichkeit, im Wege der Bild- und Tonübertragung teilzunehmen, im Gesetz zu trifft und nicht bzw. nur in engen Grenzen den Gerichten überlässt. Der Gesetzgeber könnte dazu den bereits im ArbGG und SGG beschrift-

tenen Weg noch ein Stück weitergehen und im UWG allgemein bestimmen, dass den Parteien und ihren Bevollmächtigten eine (nach wie vor freiwillige) Teilnahme im Wege der Bild- und Tonübertragung *stets* gestattet ist. Soweit es um die Vernehmung von Zeugen, Sachverständigen und Parteien geht (vgl. § 128 a II ZPO), könnte man dies um eine „Soll-Regelung“ oder eine Ausnahmeregelung ergänzen, die dem Gericht insoweit eine Möglichkeit in die Hand gibt, das „körperliche Erscheinen“ dieser Personen zu erzwingen, wenn es im Einzelfall den persönlichen Eindruck für erforderlich hält. § 14 II 4 UWG könnte insofern auch wie folgt gefasst werden:

„Für alle bürgerlichen Rechtsstreitigkeiten, mit denen ein Anspruch auf Grund dieses Gesetzes geltend gemacht wird, ist das Gericht zuständig, in dessen Bezirk der Beklagte seinen allgemeinen Gerichtsstand hat. Für alle bürgerlichen Rechtsstreitigkeiten, mit denen ein Anspruch auf Grund dieses Gesetzes geltend gemacht wird, ist außerdem das Gericht zuständig, in dessen Bezirk die Zuwiderhandlung begangen wurde.“

Den Beteiligten ist es gestattet, an Verhandlungen und Vernehmungen des Gerichts im Wege der Bild- und Tonübertragung (§ 128 a ZPO) teilzunehmen. Satz 3 gilt nicht, soweit das Gericht bei einer Vernehmung das Erscheinen des Zeugen, des Sachverständigen oder der Partei im Gerichtssaal für erforderlich hält.“

[24] Eine solche Regelung würde dann zwar auf Seiten der Gerichtsverwaltungen zu einmaligen Mehrbelastungen führen, weil die erforderliche Technik nicht mehr unter Berufung auf ein „Ausstattungsermessen“ verweigert werden könnte.³⁷ Die Belastung der Landeshaushalte hielte sich aber in engen Grenzen, weil die Kosten durch die Auslagen gem. Ziff. 9019 KV-GKG relativ zeitnah amortisiert würden und als Minimum zunächst nur die von den UWG-Kammern genutzten Säle auszustatten wären.

[25] Würde sich der Gesetzgeber zu einem solchen Schritt entschließen, wäre angesichts der eingangs geschilderten Erwägungen davon auszugehen, dass Verhandlungen in UWG-Sachen schon relativ zeitnah fast ausschließlich im Wege der Bild- und Tonübertragung stattfänden. Diskussionen über den Ort der Rechtsver-

³² BGB I 2020, 1055, sog. Sozialschutz-Paket II.

³³ Dazu LAG Düsseldorf RD i 2020, 63, m. Anm. Windau (in diesem Heft).

³⁴ Ähnlich schon Balke/Liebscher/Helwig AnwBl. 2020, 366 (368).

³⁵ So die Stellungnahme des Bundesrats im Gesetzgebungsverfahren (BR-Drucks. 245/20).

³⁶ Dazu instruktiv LAG Düsseldorf RD i 2020, 63, m. Anm. Windau (in diesem Heft), sowie zur Frage, ob die Ausstattung für die Ermessensausübung relevant sein darf, BeckOK-ZPO/von Selle, § 128 a Rn. 5.

³⁷ Eine solche Pflicht wird aber auch heute schon teilweise angenommen, s. nur BeckOK-ZPO/von Selle, § 128 a Rn. 2.2; Windau NJW 2020, 2753 Rn. 19, anders aber die h. M. unter Berufung auf die Gesetzesbegründung, s. nur Zöller/Greger, ZPO, § 128 a Rn. 1.

letzung versus den allgemeinen Gerichtsstand des Beklagten würden letztlich obsolet. Die Vorteile beider Lösungen, wenig Reiseaufwand und spezialisierte Gerichte, würden kombiniert. Damit käme der Regelung auch eine Pilotfunktion für die Einführung und Ausweitung von Online-Verfahren jenseits von UWG-Verfahren zu.

IV. Einführung eines reinen Online-Verfahrens

[26] Die Argumente für und wider den „fliegenden Gerichtsstand“ gelten nicht nur für das Lauterkeitsrecht. Im Grunde kann in allen gerichtssprengelüberschreitenden ZPO-Sachen fast jede Allokation eines Gerichtsstands zu unsachgemäßen Verhaltensanreizen führen. Liegt der Gerichtsstand am Sitz der Klägerin, führt sie dies in Versuchung, verfrüht zu klagen; liegt der Gerichtsstand hingegen am Sitz der Beklagten, hat diese einen sachwidrigen Anreiz, Ansprüche nicht zu erfüllen.³⁸ Dieses Dilemma kann im Grunde nur ein „echter“ Online-Gerichtsstand lösen, weil er Reiselasten nicht verschiebt, sondern eliminiert. Wenn man vor diesem Hintergrund darüber nachdenkt, Verhandlungen über das Maß des heutigen § 128 a ZPO hinaus in die virtuelle Sphäre zu verlagern, ist damit natürlich auch eine Reihe von Herausforderungen verbunden: Inwieweit kann man die Verfahrensbeteiligten zu einer digitalen Teilnahme am Verfahren zwingen? Wie können und sollten Kostenregelungen die Wahl zwischen klassischen und virtuellen Gerichtssälen beeinflussen? Und wie verhält es sich mit der Öffentlichkeit i. S. d. § 169 I 1 GVG im virtuellen Gerichtssaal?

1. Pflicht zur virtuellen Verhandlung?

[27] Jenseits des § 128 a ZPO ließe sich das Zivilprozessrecht ohne Weiteres dahingehend fortentwickeln, dass man für bestimmte Typen von Streitigkeiten ein reines Online-Verfahren vorsieht, in dem nicht nur die Verhandlung virtuell stattfindet, sondern der Prozess mit einer strukturierten Online-Klage initiiert und der komplette Schriftsatzverkehr anschließend digital abgewickelt wird.³⁹ Auch hier könnten UWG-Sachen eine Vorreiterrolle einnehmen; anschließend wäre etwa daran zu denken, Streitigkeiten aus dem Bereich E-Commerce oder Streitigkeiten mit Anwaltszwang als erste in den virtuellen Raum zu verlagern. Das wäre insbesondere bei solchen Verfahren sinnvoll, in denen nicht beide Parteien am selben Ort ihren Gerichtsstand haben.

[28] Ähnlich wie im Mahnverfahren könnten die Länder jeweils ein spezialisiertes Amts- oder Landgericht bestimmen, das sämtliche Verfahren eines Typs in erster Instanz bearbeitet. Damit würde auch zur Regel, was heute nur von einzelnen Großgerichten bekannt ist:

Mehrere Amtsrichter*innen bzw. Landgerichts-Kammern wären auf ein Rechtsgebiet spezialisiert und blieben damit fachlich auf Augenhöhe mit der teilweise hochspezialisierten Expertise der beteiligten Anwalt*innen, ohne dass die für die Garantie des gesetzlichen Richters notwendige Unberechenbarkeit der Geschäftsverteilung Schaden nähme.

[29] Ähnlich wie das Mahnverfahren ließe sich auch ein rein virtuelles Verfahren optional ausgestalten: Jede Klägerin hätte bei Antragstellung bzw. Klageerhebung die Wahl zwischen einem klassischen Streitverfahren und einem reinen Online-Verfahren. Letzteres wäre im Unterschied zur Lösung des § 128 a ZPO kein Ausflug ins Digitale, sondern ein Prozess auf einer genuin virtuellen Verfahrensplattform,⁴⁰ der – spiegelbildlich zum heutigen § 128 a ZPO – Ausflüge in den klassischen Gerichtssaal ermöglicht, wo die persönliche Wahrnehmung von Zeugen oder anderen Beweismitteln einmal von besonderer Bedeutung ist. Zudem könnte man beiden Parteien ähnlich wie im Mahnverfahren auch während des Prozesses die Option lassen, den Wechsel ins klassische Streitverfahren zu wählen. Es gäbe insofern keinen „Zwang in den Äther“, wohl aber eine echte und vor allem bewusste Entscheidung der Parteien für die Nutzung eines bestimmten Verfahrensmediums.

2. Kostenaspekte

[30] Sobald die Streitparteien die Wahl zwischen dem klassischen Streitverfahren und einem reinen Online-Prozess haben, wird es einerseits eine Frage des Verfahrenskomforts, andererseits aber vor allem eine Frage der Kosten sein, in welche Richtung die Praxis tendiert. Dabei versteht es sich von selbst, dass sich der Aufwand für die Beteiligten gerade bei über eine gewisse Distanz geführten Verfahren reduziert, sobald der Prozess online geführt wird.

[31] Diese Unterschiede beim Verfahrensaufwand wird man einigermaßen zwingend im Rechtsanwaltsvergütungsgesetz, ggf. auch im Gerichtskostengesetz berücksichtigen müssen.⁴¹ Das wiederum wird Folgewirkungen für die Attraktivität der verschiedenen Verfahrensspuren zeitigen. Unternehmerisch denkende Parteien werden es tendenziell bei der Nutzung des Online-Verfahrens bewenden lassen, wenn sie sich aus der Verhandlung in physischer Präsenz keine Vorteile versprechen, die von den höheren Kosten aufgewogen werden.

³⁸ Breidenbach/Glatz/Fries, RechtsHandbuch Legal Tech, 2. Aufl. 2020, Kap. 7.3 Rn. 8.

³⁹ Gaier NJW 2013, 2871 (2873 ff.); Nicolai/Wölber ZRP 2018, 229 (231 ff.); Effer-Uhe MDR 2019, 69 (70 ff.).

⁴⁰ Ein gelungenes Beispiel dafür ist etwa die Plattform des kanadischen *Civil Resolution Tribunal*, <https://civilresolutionbc.ca>; im Übrigen siehe auch die Nachweise in Fn. 39.

⁴¹ Ausführlich Fries GVRZ 2020, 27.

Auch Rechtsschutzversicherer werden das ihnen Mögliche tun, um ihre Kunden von der Nutzung unnötig aufwändiger Verfahren abzuhalten.⁴² Gegen dieses kostensensible Kalkül ist freilich nichts einzuwenden; vielmehr bringen insgesamt sinkende Verfahrenskosten sogar den Vorteil mit sich, dass die gerichtliche Rechtsdurchsetzung attraktiver wird und die Bedeutung des Rechts und der Justiz in der Gesellschaft sichtbarer wird.

3. Virtuelle Öffentlichkeit?

[32] Je mehr ein Online-Verfahren in bestimmten Rechtsgebieten zur Regel wird, desto drängender stellt sich naturgemäß die Frage nach einer angemessenen Beteiligung der Öffentlichkeit an rein virtuellen Prozessen. Die in § 169 I 1 GVG vorgesehene Öffentlichkeit der gerichtlichen Verhandlung erfüllt eine wichtige Kontrollfunktion und sichert ab, dass Urteile tatsächlich im Namen des Volkes gesprochen werden. Gerade im Zuge der COVID-19-Pandemie 2020 ist vermehrt die Sorge hörbar geworden, eine Verschiebung von Prozessen in die virtuelle Welt könnte die ohnehin schon häufig nur theoretische Öffentlichkeit vollends aus den Verhandlungssälen verbannen. Das ließe mittelfristig erhebliche Nachteile für die Akzeptanz der Justiz in der Bevölkerung befürchten.

[33] Freilich gibt es auch seit Jahren bereits sehr gehaltvolle Plädoyers dafür, die Digitalisierung des Zivilprozesses ganz bewusst zugunsten einer engeren Verbindung zwischen Justiz und Öffentlichkeit zu nutzen.⁴³ Gerade wenn man sich von dem § 128 a ZPO zugrunde liegenden Konzept einer Übertragung aus dem Gerichtssaal entfernt und Gerichtssäle genuin virtuell aufsetzt, ist es ein Leichtes, die interessierte Öffentlichkeit auch per Online-Einwahl niedrigschwellig an der Verhandlung teilhaben zu lassen. Die dagegen geäußerten Einwände stammen vorrangig nicht aus dem Zivilprozessrecht, sondern vor allem aus dem Datenschutzrecht; sie sind als solche ernstzunehmen, lassen sich aber in vielen Fällen überzeugend entkräften.⁴⁴

V. Fazit

[34] Missbräuchen des „fliegenden Gerichtsstands“ in UWG-Verfahren sollte der Gesetzgeber nicht durch dessen Einschränkung begegnen, sondern durch eine Ausweitung der Möglichkeiten, im Wege der Bild- und Tonübertragung an Gerichtsverhandlungen teilzunehmen. Für eine Ausweitung dieser Möglichkeiten im Rahmen eines Pilotprojekts bieten sich UWG-Verfahren an. Außerdem ginge damit wegen der Möglichkeiten, zeitnäher einen Termin anzuberaumen, womöglich auch eine Stärkung des rechtlichen Gehörs einher. Nach geltendem Recht sollte von den jetzt schon bestehenden Möglichkeiten des § 128 a ZPO in UWG-Verfahren ausgiebig Gebrauch gemacht werden.

[35] Zusätzlich könnte der Gesetzgeber jedenfalls den Parteien und ihren Prozessbevollmächtigten gesetzlich gestatten, an Verhandlungen in UWG-Verfahren im Wege der Bild- und Tonübertragung teilzunehmen, ohne dass es dafür einer gesonderten Entscheidung des Gerichts bedürfte. So entfielen die mit einer Anreise zu einem weit entfernten Gericht verbundenen Probleme.

[36] Mittelfristig sollte der Gesetzgeber sowohl in UWG-Sachen als auch generell in Zivilprozesssachen eine Option schaffen, das Verfahren von Beginn bis Ende komplett online zu führen. Verhandlungen in physischer Präsenz gehören nicht ins Buch der Geschichte, aber sie bringen neben vielen Vorteilen auch manche Nachteile mit sich; deswegen sollte es den Verfahrensbeteiligten in absehbarer Zeit freistehen sie abzuwählen, wo sie sie nicht benötigen.

⁴² Dass dieses „aktive Schadenmanagement“ der Rechtsschutzversicherer zuweilen im Hinblick auf ihre versicherungsvertraglichen Pflichten problematisch ist, steht auf einem anderen Blatt; weiterführend dazu *Cornelius-Winkler SVR 2013*, 201 ff.; *Cornelius-Winkler NJW 2014*, 588 (589 ff.).

⁴³ Statt vieler lesenswert *Paschke*, Digitale Gerichtsöffentlichkeit, 2018, S. 434 ff.

⁴⁴ Ausführlich *Fries GVRZ 2020*, 27 m. w. N.

Verwendung von Textbausteinen in einer Berufungsbegründung

§§ 520 III 2, § 522 I 1, 2 ZPO

Eine Berufungsbegründung, die überwiegend aus Textbausteinen besteht und sich mit dem angefochtenen Urteil nicht auseinandersetzt, genügt den Anforderungen nach § 520 III 2 ZPO nicht. (Leitsatz der Redaktion)

OLG Köln, Beschluss vom 18.8.2020 – 15 U 171/19

RA Dr. Frank Remmert*^{*}

I. Zusammenfassung des Sachverhalts

Die Klägerin macht kaufvertragliche Rückabwicklungsansprüche sowie deliktische Ersatzansprüche gegen einen namhaften Fahrzeughersteller im sog. Dieselskandal geltend. Das Landgericht Köln hat die Klage mit Urteil vom 13.6.2019 (Az. 2 O 379/18) vollumfänglich abgewiesen und im Wesentlichen damit begründet, dass ein Sachmangel i. S. v. § 434 BGB nicht schlüssig dargelegt sei. Dagegen wendet sich die Klägerin mit ihrer Berufung, mit der sie ihre erstinstanzlichen Schlussanträge – so wörtlich – „über den bereits zugesprochenen Umfang hinaus“ weiterverfolgt und sich gegen den – so wörtlich – „klageabweisenden Teil des am 20.8.2019 verkündeten Urteils“ wendet. Entsprechend §§ 513 I, 529 I Nr. 1 ZPO begründeten konkrete Anhaltspunkte Zweifel an der Richtigkeit und Vollständigkeit der erstinstanzlichen Feststellungen. Im Rahmen der 146-seitigen Berufungsbegründung erfolgen u. a. eine umfangreiche Darstellung der „Historie“ des Abgasskandals, angeblicher Mängel und Manipulationen am Fahrzeug mit anschließenden Rechtsausführungen zu einzelnen Anspruchsgrundlagen.

II. Zusammenfassung der tragenden Gründe

Das Gericht hat die Berufung nach § 522 I 2 ZPO als unzulässig verworfen, da die Berufungsbegründung den Anforderungen nach § 520 III 2 Nr. 1 bis 4 ZPO nicht gerecht werde.

Bereits im vorangegangenen Hinweisbeschluss vom 24.3.2020 hat der Senat, gestützt auf die formalen Anforderungen nach § 520 III ZPO, deutlich gemacht, dass jede Berufungsbegründung auf den konkreten Streitfall zugeschnitten sein und im Einzelnen erkennen lassen muss, aus welchen tatsächlichen und rechtlichen Gründen der Berufungskläger das angefochtene Urteil für unrichtig hält. Dazu gehöre die Angabe, welche bestimmten Punkte des angefochtenen Urteils der Berufungskläger bekämpft und welche Gründe er ihm entgegensetzt; formelhafte Wendungen und allgemeine Redewendungen genügten dabei ebenso wenig wie die pauschale Rüge, die Auffassung des Erstrichters sei

falsch oder die Anwendung einer bestimmten Vorschrift irrig. Unter Berufung auf die Rechtsprechung des BGH (*BGH NJW-RR* 2008, 1311, Rn. 11 ff.; sowie aus jüngerer Zeit *BGH*, Beschl. 22.1.2019 – XI ZB 9/18 = BeckRS 2019, 3572, Rn. 7 f. m. w. N.; *BGH*, Beschl. 25.6.2019 – XI ZB 30/18 = BeckRS 2019, 15895, Rn. 9 mwN) sowie auf weitere Entscheidungen anderer Oberlandesgerichte zum sog. Dieselskandal (so u. a. *OLG Naumburg*, Urt. 12.9.2019 – 1 U 168/18 = BeckRS 2019, 27098) führt der Senat aus, dass eine Berufungsbegründung den Anforderungen nach § 520 III ZPO nicht genüge, wenn sie weitgehend aus Textbausteinen, Urteilsversatzstücken etc. zusammengesetzt sei und auf das angefochtene Urteil nur „sporadisch“ eingehe. Textbausteinartige Darlegungen, die sich in Massenverfahren nicht vermeiden ließen, seien nur dann unschädlich, wenn sie die Subsumtion der Textbausteine auf den Einzelfall noch erkennen ließen.

Diesen Anforderungen genüge die Berufungsbegründung im konkreten Fall nach Ansicht der Kölner Richter nicht, da sie sich „bei genauem Hinsehen gar nicht“ mit dem angegriffenen Urteil befasse. Zwar sei keineswegs jede mit Textbausteinen erstellte Rechtsmittelschrift problematisch. Vorliegend fehle jedoch ein ausreichender Fallbezug. So sei bewusst eine geschlechtsneutrale Formulierung mit „Klagepartei“ gewählt worden, um die Begründung auch in anderen Verfahren verwenden zu können. Teilweise würden dem Gericht alternative Begründungen zur Auswahl geliefert. So sei zum konkreten Fahrzeug unter Beweisantritt vorgetragen, es sei „kein / ein“ (!) Ad-Blue-Tank verbaut. Der fehlende Einzelfallbezug werde auch aus weiteren Stellen in der Berufungsbegründung deutlich. So zeige sich schon ganz am Anfang der Begründung, dass offensichtlich auf ein anderes Verfahren Bezug genommen werde, wenn weder Datum noch Tenor der angefochtenen Entscheidung korrekt wiedergegeben werde. Es würden lediglich Textbausteine präsentiert in der Hoffnung, der Senat werde sich schon das Passende herausuchen.

III. Anmerkung

Das OLG Köln zeigt die haftungsrechtlichen Risiken für Rechtsanwältinnen und Rechtsanwälte auf, wenn Schriftsätze in Massenverfahren standardisiert unter Einsatz von Legal Tech-Anwendungen erstellt, die Anforderungen der ZPO dabei aber nicht eingehalten werden. Die Entscheidung geht zwar auf automatisiert generierte Schriftsätze nicht ausdrücklich ein. Massenverfahren lassen sich heute aber kaum noch ohne Einsatz spezieller Software bewältigen. Die damit einhergehen-

* Der Autor ist Rechtsanwalt und Inhaber der Kanzlei REMMERTZ LEGAL in München.

de Standardisierung und Verallgemeinerung in gleichgelagerten Fällen stehen in einem *deutlichen Spannungsverhältnis* mit dem Bestimmtheiterfordernis und dem Gebot, Sachverhalt und Gründe im Einzelfall zu konkretisieren. Die Anforderungen der ZPO gelten unabhängig davon, ob Schriftsätze individuell für einen Einzelfall oder massenhaft für viele gleichgelagerte Fälle erstellt werden. Sie sind somit auch zu beachten, wenn dies unter Einsatz von Legal Tech-Lösungen erfolgt. Die ZPO sieht insoweit keine Erleichterungen vor. Zwar ist schon seit langem anerkannt, als Legal Tech noch weitgehend unbekannt war, dass in Schriftsätzen auch Textbausteine verwendet werden können (*BGH NJW-RR* 2013, 296, Rn. 15 im Fall von Anlegerschutzprozessen; *BGH NJW-RR* 2008, 1308 – Textbausteine ohne Bezug zum Streitstoff). Es ist gleichwohl erforderlich, dass die Bestimmtheitsanforderungen der ZPO eingehalten werden. Das gilt nicht nur für eine Berufungsbegründung nach § 520 III ZPO wie im Fall des OLG Köln. Dieselben Probleme stellen sich auch in anderen Verfahren, insbesondere bei einer Klageschrift nach § 253 II ZPO (ausführlich dazu *Remmert*, AnwBl. Online 2020, 507 ff., auch zu weiteren berufs-, versicherungs- und steuerrechtlichen Risiken).

Werden die Anforderungen nach § 520 III ZPO nicht eingehalten, kann dies für die anwaltlichen Vertreter fatale haftungsrechtliche Folgen haben, da eine Heilung der Mängel nach Fristablauf nicht mehr möglich ist (*BGH*, Beschl. 25.6.2019 – XI ZB 30/18 = BeckRS 2019, 15895, Rn. 12; *OLG Frankfurt*, Urt. v. 31.7.2019 – 17 U 326/18 = BeckRS 2019, 21331).

Der Beschluss des OLG Köln ist bereits eine von mehreren obergerichtlichen Entscheidungen (neben *OLG Naumburg* (Fn. 2) u. a. auch *OLG Stuttgart*, Hinweisbeschluss v. 29.5.2017 – 5 U 46/17 = BeckRS 2017, 119632; *OLG Frankfurt*, Urt. v. 31.7.2019 – 17 U 326/18 = BeckRS 2019, 21331) in den sog. Dieselskandal-Fällen, in denen Berufungen aufgrund fehlerhafter Begründungen als unzulässig verworfen worden sind. Neben dem Problem der Standardisierung und der Verwendung von Textbausteinen dürfte hier sicher eine Rolle gespielt haben, dass die Berufungsbegründung handwerkliche Fehler aufwies. So waren u. a. Datum und Tenor der angefochtenen Entscheidung falsch wiedergegeben. Ähnliche Fehler waren auch im Fall des OLG Naumburg (*OLG Naumburg*, Urt. 12.9.2019 – 1 U 168/18 = BeckRS 2019, 27098) mit ausschlaggebend, da in der Berufungsbegründung mehrmals das LG Braunschweig erwähnt, tatsächlich aber ein Urteil des LG Magdeburg angefochten wurde. Zwischenzeitlich liegen in den Dieselskandalfällen auch erste Entscheidungen des BGH vor, die die strenge Linie der Oberlandesgerichte größtenteils bestätigen (*BGH*, Beschl. v. 21.7.2020 – VI ZB 59/19 (OLG Braunschweig bestätigt); *BGH*, Beschl. v. 25.8.2020 – VI ZB 67/19 (OLG Oldenburg bestätigt); siehe demgegenüber *BGH*,

Beschl. v. 21.7.2020 – VI ZB 7/20 (OLG Frankfurt a. M. aufgehoben; Anforderungen nach § 520 III ZPO überspannt); ebenso *BGH*, Beschl. v. 25.8.2020 – VI ZB 5/20 (ebenfalls das OLG Frankfurt a. M. betreffend)). Für Anwender von Legal-Tech-Lösungen in Massenverfahren besteht dabei die Herausforderung zu eruieren, welcher Standardisierungsgrad nach der Rechtsprechung (gerade) noch zulässig ist.

Online-Dokumentengenerator keine erlaubnispflichtige Rechtsdienstleistung i. S. d. RDG

§§ 2, 3 RDG; §§ 3, 3 a, 8 UWG

Ein digitaler Dokumentengenerator, der es dem Nutzer durch den einem Rechtsanwaltsgespräch nachempfundenen Frage-Antwort-Katalog erlaubt, auf der Basis von Textbausteinen individuelle Rechtsdokumente wie Arbeitsverträge EDV-basiert zu erstellen, stellt keine erlaubnispflichtige Rechtsdienstleistung im Sinne des § 2 RDG dar. (Leitsatz der Redaktion)

OLG Köln, Urteil vom 19.6.2020 – 6 U 263/19

Dr. Christina-Maria Leeb*

I. Zusammenfassung des Sachverhalts

Die klagende Rechtsanwaltskammer macht Unterlassungsansprüche gegen einen Verlag geltend, der – ohne im Sinne des RDG registriert zu sein – einen Legal Tech-Dienst betreibt. Die Klägerin stützt ihre Ansprüche einerseits auf behauptete Verstöße gegen §§ 2, 3 RDG (i. V. m. §§ 8 I, III Nr. 3; 3 I; 3 a UWG) und andererseits auf irreführende Werbeaussagen (§ 5 UWG). Der streitgegenständliche Dienst ist ein unter dem Namen „Smartlaw“ vertriebener Online-Dokumentengenerator, worüber sich Privatpersonen und Unternehmen nach einem Frage-Antwort-Dialog juristische Dokumente verschiedenster Art zusammenstellen und herunterladen können – von Arbeitsverträgen über eine unternehmensinterne Richtlinie zur Nutzung von Social Media bis hin zur Kündigung des Fitnessstudios.

Die monierten Werbeaussagen kennzeichnen als verbindendes Element, dass das beworbene Internetangebot hiernach mit individueller anwaltlicher Arbeit qualitativ auf Augenhöhe stünde und in Bezug auf Kosten und Schnelligkeit der Lieferung dem sogar noch überlegen sei.

II. Zusammenfassung der tragenden Gründe

Das OLG Köln ändert die erstinstanzliche Entscheidung des LG Köln dahingehend ab, als dass es einen Unterlassungsanspruch lediglich hinsichtlich der Werbeaussagen

* Die Autorin ist Wissenschaftliche Mitarbeiterin bei der HEUSSEN Rechtsanwalts-gesellschaft mbH in München.

bejaht. Im Übrigen – und damit in Bezug auf das Geschäftsmodell als solches – weist es die Klage als unbegründet ab, nachdem die Beklagte mit dem Dokumentengenerator keine erlaubnispflichtige Rechtsdienstleistung i. S. d. §§ 2 I, 3 RDG erbringe. Nach dem OLG liegen die Tatbestandsmerkmale einer Tätigkeit in konkreten fremden Angelegenheiten, die eine Prüfung des Einzelfalls erfordert, nicht vor.

In seiner Begründung stellt das Berufungsgericht als denkbare Tätigkeit des Dienstleisters zum einen auf die Programmierung und Bereitstellung des Dokumentengenerators ab. Diese stelle allerdings schon keine erlaubnispflichtige Rechtsdienstleistung dar, da sie nicht in konkreten Angelegenheiten erfolge und überdies jedenfalls keine Einzelfallprüfung erfordere. Zum anderen komme zwar noch die Anwendung des Generators durch die Nutzerin bzw. den Nutzer in Betracht. Hier fehle es – so das OLG Köln – allerdings an einer Zurechnung dieser Tätigkeit an die Beklagte. Eine solche ergebe sich insbesondere nicht durch Eröffnung einer Gefahrenquelle im Schutzbereich des RDG, nachdem der Dokumentengenerator keine Gefahr begründe, vor die das RDG schützen solle. Zentral ist dabei der Ausgangspunkt des Gerichts, dass angesichts der immer weiter zunehmenden Verrechtlichung des Alltagslebens und der ständigen Entwicklung neuer Dienstleistungsberufe – auch im Rechtsbereich – der Verbotsbereich des RDG auf Fälle „echter Rechtsanwendung“ beschränkt bleiben müsse. Eine solche sei allerdings bei einem rein schematisch ablaufenden Subsumtionsvorgang auf Basis vorgegebener Ja-/Nein-Entscheidungsstrukturen – wie bei dem Dienst der Beklagten – nach Auffassung des OLG nicht gegeben.

Das Berufungsgericht führt darüber hinaus noch aus, dass es dahinstehen könne, ob eine erlaubnispflichtige Rechtsdienstleistung bei dem Einsatz sog. Künstlicher Intelligenz in Betracht komme.

Die zugelassene Revision ist derzeit beim BGH unter dem Az. I ZR 113/20 anhängig.

III. Anmerkung

Mag man unter der Vielzahl an Entscheidungen aus 2020 zum Themenbereich Legal Tech (im engeren Sinne) ein Zwischenfazit ziehen, so ist die dargestellte Entscheidung des OLG Köln vermutlich als die bisher bedeutendste für die Rechtspraxis anzusehen. Weitete der BGH seine zur Reichweite der in § 10 I Satz 1 Nr. 1 RDG normierten Inkassoerlaubnis (*BGH NJW 2020, 208* – „wenigermiete.de I“) gefasste, liberale Rechtsprechung zugunsten nichtanwaltlicher Rechtsdienstleistungen und mithin einem entwicklungs-offenen RDG weiter aus – wovon auszugehen ist –, erlebt die noch junge Legal Tech-Branche sicherlich weiteren Aufwind.

Die ausführlich begründete und bislang in der Literatur auch überwiegend positiv aufgenommene (vgl. *Decken-*

*brock DB 2019, 1563; Stein/Ruppert DStR 2020, 2040; differenzierend Henssler/Flory EWiR 2020, 495 (496); Römermann NJW 2020, 2678 (2679 ff.); Wessels MMR 2020, 621 f.) Entscheidung des OLG Köln fügt sich in ihrem Kerngehalt in die bisherige, auch bereits vor „wenigermiete.de“ ergangene Rechtsprechung ein, wenngleich auch der streitgegenständliche Dienst vermutlich mit dem höchsten Grad an Komplexität und Individualität ausgestattet ist, über den bislang ein Gericht mit Blick auf das Vorliegen einer erlaubnispflichtigen Rechtsdienstleistung je zu befinden hatte. Bei §§ 2, 3 RDG ist insoweit maßgeblich am Erfordernis einer – einzelfallbezogenen – Rechtsprüfung anzuknüpfen (ebenso *Wessels MMR 2020, 621 (622)*). Hierbei versucht die Rechtsprechung seit geraumer Zeit, die naturgemäß unscharfe Trennlinie am Maßstab der Verkehrsanschauung oder der erkennbaren Erwartung des bzw. der Rechtsuchenden zwischen einer objektiv erforderlichen, substantiellen bzw. vertieften Rechtsprüfung und einer lediglich einfachen oder schematischen Rechtsanwendung zu ziehen (vgl. etwa *BGH GRUR 2011, 539 (542); BSG NJW 2014, 493 (494); BGH NJW-RR 2016, 1056 (1060); BGH NJW 2016, 3441 (3443)*). Dass dies naturgemäß typischerweise noch auf Basis von Vorläufern der Online-Dokumentengeneratoren – und weiteren analogen Entsprechungen zur heutigen digitalen Welt – geschah, verdeutlicht etwa eine Entscheidung des OLG Karlsruhe aus 2010: Hiernach ist eine solche Rechtsprüfung dann nicht erforderlich, wenn lediglich ein standardisiertes – papiernes – Vertragsformular ohne rechtliche Hilfestellung beim Ausfüllen zur Verfügung gestellt wird (*OLG Karlsruhe NJW-RR 2011, 119 (120)*).*

Die Besprechungsentscheidung deutet es in ihrem Nebensatz zur KI bereits an: Je technisch komplexer und ausgereifter die Tools unter Zugrundelegung ihrer Funktionsweise im Einzelfall werden, desto näher wird die Annahme eines objektiven Erfordernisses einer einzelfallbezogenen Rechtsprüfung durch den Dienst selbst rücken müssen. Dabei darf diese allerdings in Zukunft nicht vorschnell unter dem Schlagwort der Künstlichen Intelligenz bejaht werden. Jedenfalls bei dem Einsatz selbstlernender Algorithmen mit entsprechendem Grad an Eigenständigkeit mag dies zukünftig für „rechtsberatende künstliche Intelligenzen“ anzunehmen sein (vgl. *Kaulartz/Braegelmann/Fries, Rechtshandbuch Artificial Intelligence und Machine Learning, 2020, 651 (656)*; anders wohl *Römermann NJW 2020, 2678 (2682)*, wonach es auch bei dem Einsatz von KI stets am Einzelfall fehle). Dabei wird u. U. auch ein besonders umfangreicher Smart Contract unter den Begriff der erlaubnispflichtigen Rechtsdienstleistung zu subsumieren sein (in diese Richtung bereits *Taeger/Kaulartz, Tagungsband DSRI Herbstakademie 2016, 1023 (1033)*, der allerdings hierbei noch maßgeblich auf die Programmier-tätigkeit abstellt). Dem gegenüber stehen noch die gegenwärtig am deutschen Markt verfügbaren Lösungen,

etwa in Gestalt von Chatbotlösungen in der Beratung, die – soweit ersichtlich – noch nicht mehr als standardisierte Antworten auf vorgegebene Fragen liefern (hierzu *Leeb*, Digitalisierung, Legal Technology und Innovati-

on, 2019, S. 253 ff.). Dass sich dies angesichts des rasanten Fortschritts der technologischen Entwicklung in und außerhalb des Rechtsberatungsmarktes bald ändern wird, ist allerdings gewiss.

E-JUSTICE/E-GOVERNMENT

Anforderungen an die Bearbeitbarkeit eines elektronischen Dokuments gem. § 130 a II ZPO

§ 130 a II 1 ZPO, § 2 I ERVV

Allein der Verstoß gegen die Vorgaben zum Dateiformat führt nicht dazu, dass die elektronisch eingereichte Berufungsbegründung (hier: in DOCX-Format) nicht zur Bearbeitung bei Gericht geeignet ist. (Leitsatz der Redaktion)

LG Mannheim, Urteil vom 4.9.2020 – 1 S 29/20

DirSG Dr. Henning Müller*

I. Zusammenfassung des Sachverhalts

In einem Rechtsstreit über die zivilrechtlichen Ansprüche aus einem Verkehrsunfall reichte der Berufungskläger die Berufungsbegründung im Format DOCX ein. Das Landgericht Mannheim führt die Gerichtsakte bereits elektronisch.

II. Zusammenfassung der tragenden Gründe

Das Gericht sah die Berufungsbegründung als formwirksam an, obwohl sie nicht als PDF- oder TIFF-Datei eingereicht wurde. Die Berufungskammer habe in ihrer elektronischen Akte mit dem Repräsentat des elektronischen Dokuments ohne Weiteres arbeiten können. Die elektronischen Dokumente im eingereichten Format würden im Hintergrund dieser Repräsentate gespeichert; nur im Bedarfsfall würde auf die Originaldatei zurückgegriffen. Das Repräsentat wiederum sei eine PDF/A-Datei. Die Konvertierung der eingereichten DOCX-Datei in das Repräsentat sei problemlos erfolgt.

Allein der Verstoß gegen die Vorgaben zum Dateiformat durch § 130 a II 2 ZPO iVm. § 2 I ERVV führe noch nicht dazu, dass das elektronische Dokument nicht zur Bearbeitung im Sinne des § 130 a II 1 ZPO geeignet gewesen sei. Die technischen Rahmenbedingungen für die Bearbeitung nach § 130 a II 2 ZPO iVm der ERVV konkretisierten die Geeignetheit nach § 130 a II 1 ZPO, beschränkten diese jedoch nicht. Der ERVV und den ERVB komme insbesondere die Bedeutung zu, dass die Justiz in ihrem Umfang eine Bearbeitbarkeit innerhalb ihrer IT-Systeme garantiere. Reiche ein Verfahrensbetei-

ligter Dokumente in einem anderen Dateiformat ein, handele er insoweit auf eigene Gefahr. Es bestehe kein Anspruch eines Verfahrensbeteiligten, dass die Justiz mit einem elektronischen Dokument arbeiten könne, das nicht diesen technischen Rahmenbedingungen entspreche.

Entscheidend sei allein, ob das adressierte Gericht mit dem eingereichten elektronischen Dokument tatsächlich arbeiten könne. Der Maßstab der „subjektiven Eignung“ ergebe sich bereits aus dem Wortlaut. Auf die Bearbeitbarkeit durch andere Gerichte oder Verfahrensbeteiligte komme es hingegen nicht an. Dies seien bloß Folgefragen des Akten- oder Dokumentenversands.

Wollte man alle Einzelheiten der technischen Rahmenbedingungen prüfen, würde dies nicht nur die Kompetenzen der Richterschaft und die Leistungskapazitäten der Justiz strapazieren. Vielmehr sei die Prüfung auch nutzlos: Denn könne das Gericht faktisch mit dem elektronischen Dokument arbeiten, sei der Zweck der technischen Rahmenbedingungen auf andere Weise erreicht. Hierfür spreche auch die Rechtsprechung des BVerfG zu prozessualen Formvoraussetzungen im Lichte der Garantie des effektiven Rechtsschutzes nach Art. 19 IV GG, sowie nach Art. 2 I GG iVm dem Rechtsstaatsprinzip (*BVerfG* NJW 2005, 814). Danach dürfe der Zugang zu den Gerichten durch Anforderungen des formellen Rechts nicht in unverhältnismäßiger Weise erschwert werden. Dies sei aber der Fall, wenn ein für die Bearbeitbarkeit durch das Gericht faktisch folgenloser Verstoß gegen die ERVV zu einer Unwirksamkeit des Eingangs führen würde.

III. Anmerkung

Nach der bis zum 31.12.2017 gültigen Fassung bezogen sich die dort definierten besonderen Anforderungen an Dateitypen oder die Notwendigkeit einer qualifizierten elektronischen Signatur nur auf Dokumente, für die „die Schriftform vorgesehen ist“. Dies ist vor allem also bei bestimmenden Schriftsätzen der Fall, im Übrigen (also bspw. bei Anlagen zu Schriftsätzen, bei Sachverständigengutachten etc.) aber nicht. § 130 a I-3 ZPO in der seit 1.1.2018 gültigen Fassung verschärft ausweislich seines Wortlauts diese Voraussetzungen. Ab diesem

* Der Autor ist Direktor des Sozialgerichts in Darmstadt.

Zeitpunkt „müssen“ (explizit genannt) Anlagen, Gutachten etc. die besonderen Formvorschriften des elektronischen Rechtsverkehrs beachten. Eine eindeutige Rechtsfolge dieser erweiterten Rechtspflicht zur Einhaltung von Formvorschriften enthält das Gesetz allerdings nicht (mehr).

1. Schriftformwahrung

§ 130 a ZPO und die ERVV formulieren mithin keine explizite Sanktion bei Verstößen (a.A. GK-ArbGG/*Horcher* (Stand: 4.9.2020), § 46 c ArbGG Rn. 31: Wortlaut liefert klaren Hinweis, dass das Dokument nicht wirksam eingereicht wurde). Naheliegend ist, dass Vorschriften, die den Formanforderungen des § 130 a ZPO und der ERVV i. V. m. ERVB nicht genügen, jedenfalls eine prozessrechtlich oder materiell-rechtlich vorgesehene Schriftform nicht wahren. So scheint auch die bislang herrschende Meinung zu verfahren. Insoweit zitiert das LG Mannheim beispielhaft das ArbG Lübeck (*ArbG Lübeck NZA 2020, 970*). Letztlich wird diese Linie aber auch mehr oder minder unausgesprochen von sämtlichen Bundesgerichten verfolgt; zuletzt vom BAG (*BAG NJW 2020, 3192; NZA 2018, 1214*), aber jedenfalls im Rahmen der sog. Containersignatur-Rechtsprechung auch von zahlreichen anderen Gerichten (*BGH NJW 2019, 2230; BSG MMR 2019, 61; BVerwG NVwZ 2018, 1880*).

Das LG Mannheim legt insoweit zu Recht den Finger in die Wunde, dass die vollständige Prüfung sämtlicher – teilweise durchaus kleinteiliger – Anforderungen der ERVV und der ERVB die Ressourcen richterlicher Arbeitskraft insbesondere in den hochbelasteten ersten Instanzen unverhältnismäßig bindet. Beispielhaft verdeutlicht den Umfang der dann notwendigen Prüfungsdichte eine Entscheidung des LAG Frankfurt am Main zur Einbettung von Schriftarten (*LAG Frankfurt am Main, BeckRS 2020, 23235*).

2. Verhältnismäßigkeitserwägungen

Unter Berücksichtigung der Rechtsprechung des Bundesverfassungsgerichts (*BVerfG NJW 2005, 814*) spricht deshalb mit dem auch vom LG Mannheim gefundenen Ergebnis vieles dafür, dass eine starre Rechtsfolge für die Formvoraussetzungen der ERVV und ERVB nicht formuliert werden kann, sondern es stets einer Verhältnismäßigkeitsabwägung bedarf (so auch *Müller*, eJustice-Praxishandbuch, 5. Aufl. 2020, S. 132 ff.; *jurisPK-ERV/Müller*, § 130 a ZPO Rn. 41 ff.; a. A. GK-ArbGG/*Horcher*, § 46 c ArbGG Rn. 49).

In einer solchen Abwägung spricht zugunsten der Unzulässigkeit einer Einreichung eines elektronischen Dokuments, das nicht der Form der ERVV/ERVB entspricht:

- Die Einreichung ist nicht lesbar, nicht zu öffnen oder nicht der (elektronischen) Akte des Gerichts hin-

zufügbar (bspw. defekte/korrupte Datei, Virenbefall, exotisches Dateiformat).

- Die Einreichung gefährdet die IT-Sicherheit des Gerichts oder des Verfahrensgegners (bspw. für Schadsoftware anfälliges Dateiformat, aktive Inhalte der Datei).
- Die Datei ist passwortgeschützt (auch bei bekanntem Passwort), nicht druckbar oder nicht kopierbar, weshalb die Weiterverarbeitbarkeit in der elektronischen Gerichtsakte oder in einer Papiergerichtsakte erheblich erschwert wird.

Im Rahmen einer Abwägung kann im Ergebnis die Einreichung eines elektronischen Dokuments, das nicht der Form der ERVV/ERVB entspricht, aber auch zulässig sein, wenn:

- das elektronische Dokument prozessrechtlich oder materiell-rechtlich nicht der Schriftform unterlag und faktisch für das Gericht lesbar war (bspw. eine Anlage zu einem Schriftsatz),
- das elektronische Dokument nur eine „Soll-Vorschrift“ der ERVV/ERVB verletzt (bspw. § 2 II, 3 ERVV),
- das elektronische Dokument zwingende Vorschriften der ERVV/ERVB verletzt, die aber bloße Ordnungsvorschriften darstellen, weil eine Weiterverarbeitung nur unwesentlich erschwert wird (bspw. fehlende Texterkennung (a.A. *BAG NJW 2020, 1694*)).

Es ist im Übrigen im Hinblick auf den Wortlaut fraglich, ob die Verordnungsermächtigung des § 130 a II 2 ZPO die Bestimmung zwingender Formvorschriften auch dann deckt, wenn sie nur Komfortfunktionen bei der Weiterverarbeitung dienen (bspw. Texterkennung) und die Bearbeitbarkeit des Dokuments selbst nicht betreffen. Diesen Gedanken konsequent fortentwickelnd kann man tatsächlich zu dem – allerdings sehr weitgehenden – Ergebnis des LG Mannheim kommen, dass letztlich jeder Formverstoß gegen die ERVV/ERVB folgenlos bleibt, wenn das Gericht tatsächlich mit dem eingereichten Dokument umgehen kann. Ob man allerdings so weit gehen kann, dass man Probleme der Bearbeitbarkeit anderer Verfahrensbeteiligter und Gerichte als reine Folgefragen gänzlich außer Acht lässt, muss die weitere Entwicklung der Rechtsprechung noch zeigen. Es liegt nahe, dass sich auch das BVerfG insoweit noch in die Untiefen des elektronischen Rechtsverkehrs begeben muss, um seine bisherige Rechtsprechung zu konkretisieren und zu modernisieren.

Bereits nicht anwendbar sind schließlich die Formvorschriften der ERVV und der ERVB auf elektronische Dokumente, die nicht als Schriftsatz, sondern als Beweismittel eingereicht werden. Dies können bspw. auch elektronisch eingereichte Anlagen zu Schriftsätzen sein oder in den öffentlich-rechtlichen Verfahrensordnungen beigezogene elektronische Behördenakten.

Nachhall für die Praxis sollte aber die Mahnung des LG Mannheim haben, dass der Einreicher letztlich selbst bei großzügigster Auslegung der Formvorschriften nur dann eine Garantie hat, dass seine Einreichung wirksam war, wenn er sich an die Vorgaben der ERVV/ERVB hält. DOCX-Nutzer fahren einen höchst gefährlichen Kurs. Ihre Rettung kann ggf. allenfalls noch § 130 a VI ZPO. Die hierzu ergangene Rechtsprechung vor allem des BGH (BGH NJW 2019, 2230 mit krit. Anm. Müller FA 2019, 198) ist aber durchaus streng. Wer das Risiko nicht liebt, sollte daher konsequent PDF/A (Müller, eJustice-Praxishandbuch, S. 121 ff.) nutzen und auch auf die Texterkennung der eingereichten Schriftsätze achten.

Grundsatz des fairen Verfahrens – nicht gespeicherte Messdaten

§§ 46 I, 77 II Nr. 1, 79 III OWiG; § 338 Nr. 8 StPO

„Das Recht auf ein faires Verfahren gebietet es nicht, dass für den Betroffenen eine anlasslose Überprüfung des Messergebnisses in jedem Fall gewährleistet sein muss mit der Folge, dass der Umstand, dass im Rahmen des Messverfahrens die Rohmessdaten nicht gespeichert werden und daher insoweit für eine nachträgliche Richtigkeitskontrolle der Messung nicht zur Verfügung stehen, nicht grundsätzlich gegen das Gebot des fairen Verfahrens verstößt.“ (Rn. 5) (Leitsatz der Redaktion)

OLG Hamm (3. Senat für Bußgeldsachen),
Beschluss vom 25.11.2019 – 3 RBs 307/19

Prof. Dr. Thomas Wischmeyer/Oskar Schumacher*

I. Zusammenfassung des Sachverhalts

Das Amtsgericht Herford hat den Betroffenen wegen fahrlässiger Überschreitung der zulässigen Höchstgeschwindigkeit zu einer Geldbuße verurteilt und ihm unter Gewährung von Vollstreckungsaufschub verboten, Kraftfahrzeuge jeder Art im öffentlichen Straßenverkehr zu führen. Der Geschwindigkeitsverstoß wurde festgestellt mittels eines Messgeräts der Marke TraffiStar S 350, welches keine Rohmessdaten der Geschwindigkeitsmessung speichert. Das Messgerät war von der Physikalisch-Technischen Bundesanstalt (PTB) zugelassen und verwendet ein standardisiertes Prüfverfahren zur Geschwindigkeitsmessung.

II. Zusammenfassung der tragenden Gründe

Das Gericht hat die Rechtsbeschwerde als unbegründet verworfen, da die Nachprüfung des Urteils keinen Rechtsfehler zum Nachteil des Betroffenen ergeben habe. Das Gericht führt aus, dass entgegen der Entscheidung des Verfassungsgerichtshofs des Saarlandes

(VerfGH Saarland, NJW 2019, 2456) in der fehlenden Speicherung der Rohmessdaten kein Verstoß gegen den Grundsatz des fairen Verfahrens liege, vielmehr überdehne diese Entscheidung dieses rechtsstaatliche Prinzip.

Das Recht auf ein faires Verfahren solle dem Betroffenen die Möglichkeit geben, zur Wahrung seiner Rechte auf das Verfahren Einfluss nehmen zu können und setze daher einen Mindestbestand an Mitwirkungsbefugnissen voraus. Das Ordnungswidrigkeitenverfahren sei wie das Strafverfahren als ein vom Prinzip der materiellen Wahrheitserforschung beherrschter Amtsprozess ausgestaltet. Der Betroffene könne daher nur bedingt auf Inhalt und Umfang der gerichtlichen Sachaufklärung Einfluss nehmen. Dies zeige insbesondere § 77 II Nr. 1 OWiG, wonach ein Beweisantrag abgelehnt werden könne, wenn nach pflichtgemäßem Ermessen die Beweiserhebung zur Erforschung der Wahrheit nicht erforderlich ist. Anders als das Strafverfahren, in dem es um die Ahndung kriminellen Unrechts gehe und in dem im Falle einer Verurteilung ein sozialetischer Tadel ausgesprochen werde, gehe es zudem im Bußgeldverfahren allein um die Ahndung von Ungehorsam gegenüber verwaltungsrechtlichen Vorgaben. Dies lasse weitergehende Verfahrensvereinfachungen zu. Solche Vereinfachungen seien zudem geboten mit Blick auf die absolute Verjährungsfrist und den Charakter gerade von Verkehrsordnungswidrigkeitenverfahren als Massenverfahren des täglichen Lebens, die sich durch eine geringe Eingriffsintensität der Sanktion auszeichneten.

Dem im Bußgeldverfahren geltenden Effizienzbedürfnis werde im Fall von Geschwindigkeitsverstößen insbesondere durch die Anerkennung von sog. standardisierten Messverfahren Rechnung getragen. Die amtliche Zulassung von Geräten und Methoden als Voraussetzung für die Qualifikation des Messverfahrens als „standardisiert“ verfolge wie die Reduzierung des gemessenen Wertes um einen Toleranzwert den Zweck, Verwaltungsbehörden und Gerichte von der Sachverständigenbegutachtung und Erörterung des Regelfalls frei zu stellen. Ist somit ein Messgerät von der PTB zugelassen und ist es im Rahmen der Zulassungsvorgaben verwendet worden, müsse das Tatgericht grundsätzlich keine weiteren technischen Prüfungen vornehmen. Die Zulassung durch die PTB als antizipiertes Sachverständigengutachten ersetze diese Prüfung. Etwas anderes gilt nur dann, wenn der Einzelfall zur Überprüfung des Messergebnisses Anlass gibt, weil konkrete Anhaltspunkte für eine fehlerhafte Messung vorliegen. Angesichts der dargestellten Strukturelemente des Bußgeldverfahrens hält es das Gericht nicht für geboten, dass für den Betroffenen eine anlasslose Überprüfung des Messergebnisses aufgrund der Rohmessdaten in jedem Fall gewährleistet

* Der Autor Wischmeyer ist Inhaber des Lehrstuhls für Öffentliches Recht und Recht der Digitalisierung an der Universität Bielefeld. Der Autor Schumacher ist Wissenschaftlicher Mitarbeiter ebendort.

sein müsse, mit der Folge, dass der Umstand, dass im Rahmen des Messverfahrens die Rohmessdaten nicht gespeichert werden und daher insoweit für eine nachträgliche Richtigkeitskontrolle der Messung nicht zur Verfügung stehen, nicht grundsätzlich gegen das Gebot des fairen Verfahrens verstoße.

Soweit der VerfGH Saarland seinen Ansatz auf das Urteil des Bundesverfassungsgerichts zu elektronischen Wahlgeräten stütze (*BVerfG*, BVerfGE 123, 39), vermöge dies nicht zu überzeugen, da Prüfungsmaßstab dieser Entscheidung der Grundsatz der Öffentlichkeit der Wahl gewesen sei, woraus keine zu verallgemeinern den Anforderungen zu ziehen seien.

Schließlich greife auch das Argument des VerfGH Saarland, der Bürger würde durch eine Verweisung darauf, dass alles schon seine Richtigkeit habe, zum unmündigen Objekt staatlicher Verfügbarkeit gemacht und der amtlichen Bestätigung der Zuverlässigkeit eines elektronischen Systems und der es steuernden Algorithmen ausgeliefert, im Ergebnis nicht durch. Vielmehr stünden dem Bürger nach wie vor die Rechte zur Verfügung, über die auch der Angeklagte in einem gegen ihn geführten Strafverfahren verfügt, wie Akteneinsicht oder das Recht, konkrete Zweifel an der Zuverlässigkeit der Messung vorzutragen oder mittels seines Fragerechts mitzuwirken. Schließlich könne er gemäß § 39 I MessEG bei der zuständigen Landesbehörde eine Befundprüfung beantragen und sich auf diesem Wege Klarheit darüber verschaffen, ob das jeweilige Messgerät den Anforderungen der Eichung und der Konformitätsprüfung genügt. Liefere auch diese Befundprüfung keine Anhaltspunkte für eine Fehlerhaftigkeit des Messgerätes, bestehe für das Amtsgericht, soweit es sich um ein standardisiertes Messverfahren handele, keine weitere Veranlassung, das Messergebnis in Frage zu stellen und einer technischen Nachprüfung zu unterziehen.

Die Forderung des VerfGH Saarland orientiere sich somit nicht an dem verfassungsrechtlich geforderten Mindestmaß, sondern fordere das maximal Mögliche. Dies sei mit Blick auf die strukturellen Ausprägungen des Bußgeldverfahrens und deren regelmäßig geringe Eingriffstiefe verfassungsrechtlich nicht geboten.

III. Anmerkung

Die Entscheidung des OLG Hamm gewinnt ihre Bedeutung in erster Linie daraus, dass sie sich einreihet in eine Folge obergerichtlicher Entscheidungen, die sich gegen das Urteil des VerfGH Saarland wenden (vgl. jüngst auch *OLG Bremen*, BeckRS 2020, 5935). In dieser Entscheidung war in Aufsehen erregender Weise die Verwertung der Ergebnisse bestimmter Messanlagen im Bußgeldverfahren untersagt worden. Zur Begründung hatte das Gericht darauf verwiesen, dass der Einsatz algorithmischer Systeme in der (Ordnungs-)Verwaltung aus Gründen der Rechtsstaatlichkeit und des fairen Ver-

fahrens nur dann zulässig sei, wenn diese Systeme umfassend transparent wären.

Die daran anschließende Diskussion beschränkte sich denn auch nicht auf Fragen des Verkehrsrechts, sondern sah in der Entscheidung einen ersten Versuch, allgemeine Leitlinien für den Einsatz algorithmischer Systeme in der (Eingriffs-)Verwaltung zu formulieren. Es erscheint jedoch mit dem OLG Hamm nicht überzeugend, derart weitreichende Anforderungen an den Einsatz der teilweise „opaken“ Systeme zu stellen.

Dies beginnt bereits bei der Maßstabsbildung: Soweit der VerfGH Saarland aus der Entscheidung des BVerfG zum Einsatz elektronischer Wahlgeräte (*BVerfG* BVerfGE 123, 36) herleitet, dass Rechtsstaatlichkeit die „Transparenz und Kontrollierbarkeit jeder staatlichen Machtausübung“ verlange, verallgemeinert er diese Feststellung in überschießender Weise. So wird für den herausgehobenen und in seiner legitimierenden Funktion sensiblen Akt der Wahl – gerade auch im Lichte jüngerer Erfahrungen mit der Sicherheit staatlicher IT-Systeme – gelten, dass eine vorgelagerte technische Kontrolle der Wahlgeräte nicht ausreicht. Hier muss stets nachvollzogen werden können, wie das System im Einzelfall operiert hat, wofür es auch der Rohdaten bedarf. Im hier gegenständlichen Bußgeldverfahren gilt jedoch – so zu Recht das OLG Hamm – anderes. Hier handelt es sich um ein Massenverfahren von relativ geringer Eingriffstiefe. Als solches ist es nach hergebrachten Grundsätzen vor dem Hintergrund rechtsstaatlicher Effizienzgebote in gesetzlich zu determinierendem Umfang für Typisierungen und Pauschalisierungen offen. Dadurch dürfen zwar geschützte Rechtspositionen Beteiligter nicht übermäßig verkürzt werden. Dem Gesetzgeber sind insoweit im Eingriffsverwaltungsrecht durchaus Grenzen gesetzt, die auch enger zu ziehen sind als in der wohl tendenziell automationsgeeigneteren Leistungsverwaltung. Dennoch bleiben Typisierungen möglich. Entsprechend muss es dann beim Einsatz technischer Systeme möglich sein, auf sog. standardisierte Messverfahren zurückzugreifen, sofern diese dem Bedürfnis nach Verfahrensvereinfachung Rechnung tragen, ohne auf hinreichende rechtsstaatliche Absicherung zu verzichten. Insofern vermag dann auch der Verweis auf den Grundsatz des fairen Verfahrens oder der Einwand, darin liege eine Herabwürdigung des Betroffenen zum „Objekt“, nicht zu überzeugen. Vielmehr genügt in diesen Fällen, wie das OLG Hamm richtig ausführt, die Möglichkeit des Antrags auf Befundprüfung gem. § 39 MessEG i. V. m. § 39 MessEV.

Die Erwägungen des OLG Hamm weisen den Weg zu einem rechtsstaatlich angemessenen Umgang mit algorithmischen Systemen in der Verwaltung. Die Antwort auf neuartige Fehler- und Problemdimensionen dürfte weniger in einer pauschalen Erhöhung der konkreten Anforderungen zu suchen sein, deren rechtsstaatlicher Nutzen ebenso unklar bleibt wie der verfahrensmäßige

Gewinn für den Betroffenen. Vielmehr ist es geboten, die Lösung für die sich hier stellenden Fragen im systemischen Zusammenwirken der bereits durch die Rechtsordnung aufgegebenen Instrumente zu suchen. Dies kann im Falle fehlender Transparenz unter Rückgriff auf bestehende – wenn auch sicherlich nicht in jeder Konstellation hinreichend ausgereifte – Mechanismen der risikoadäquaten (und gesetzgeberisch determinierten) selektiven Vorverlagerung des rechtstaatlichen Prüfverfahrens gelingen. Im vorliegenden Fall ist also die konkrete Tauglichkeit einer Rechtsfigur wie der des „standardisierten Messverfahrens“ nicht grundlos in Frage zu stellen.

Zugleich ist aber aus rechtsstaatlicher Sicht selbstverständlich, dass entsprechende Mechanismen stets überprüft und gegebenenfalls auch fortentwickelt werden müssen. Konkret bedeutet dies, dass ein (Rechts-)Weg gegeben sein muss, auf dem sich die grundsätzlichen Feststellungen und Annahmen des vorverlagerten Verfahrens konkret hinterfragen und prüfen lassen, wie es hier durch die Möglichkeit der „Befundprüfung“ eröffnet ist. Die konsequente Einbettung algorithmischer Systeme in entsprechende (und vielfach bereits bestehende) Prüf- und Kontrollzusammenhänge ermöglichen es, den Einsatz solcher Systeme rechtsstaatlich konstruktiv einzuhegen und ihr Potential unter Wahrung der verfahrensrechtlichen Positionen nutzbar zu machen.

Zur Anfechtbarkeit der Ablehnung einer Videokonferenzverhandlung

§§ 128 a I, II, III 3; 567 I Nr. 1, 2, II ZPO, § 114 I 3, III ArbGG, §§ 110 a III 2, 211 I 3, III SGG

Die gerichtliche Anordnung oder Versagung einer Verhandlung im Wege der Bild- und Tonübertragung im Falle einer Pandemie gem. § 114 ArbGG (ebenso § 211 SGG) ist nicht anfechtbar. (Amtlicher Leitsatz)

LAG Düsseldorf, Beschluss vom 2.7.2020 – 4 Ta 200/20

RiLG Benedikt Windau*

I. Zusammenfassung des Sachverhalts

Die Klägerin in einem Kündigungsschutzprozess vor dem Arbeitsgericht Düsseldorf hatte beantragt, ihr während des auf den 9.7.2020 anberaumten Gütetermins gem. § 114 III 1 ArbGG zu gestatten, sich in den Kanzleiräumen ihrer Prozessbevollmächtigten in Hamburg aufzuhalten. Dazu verwies sie auf die zu diesem Zeitpunkt sehr hohe Zahl an Covid-19-Neuinfektionen in den Kreisen Gütersloh und Warendorf.

Das Arbeitsgericht wies den Antrag mit Beschluss vom 2.7.2020 zurück und begründete dies im Wesentlichen damit, dass die dafür erforderliche Technik nicht zur Verfügung stehe, privat

beschaffte Technik nicht genutzt werden dürfe und ausreichende Schutzmaßnahmen im Gericht vorhanden seien.

Dagegen wendete sich die Klägerin mit ihrer sofortigen Beschwerde.

II. Zusammenfassung der tragenden Gründe

Das LAG hat die sofortige Beschwerde mangels Statthaftigkeit als unzulässig verworfen und dazu die Regelung in § 128 a III 2 ZPO entsprechend herangezogen.

Die sofortige Beschwerde sei zwar grundsätzlich gemäß § 567 I Nr. 2 ZPO statthaft, da die Entscheidung des Arbeitsgerichts gemäß § 114 III ArbGG eine mündliche Verhandlung nicht erforderte und ein das Verfahren betreffendes Gesuch zurückgewiesen habe, nämlich der Klägerin zu gestatten, den Termin an einem anderen Ort bei zeitgleicher Bild- und Tonübertragung wahrzunehmen. Die sofortige Beschwerde sei hier aber abweichend von der allgemeinen Regelung in § 567 I Nr. 2 ZPO gemäß § 128 a III 2 ZPO ausdrücklich ausgeschlossen.

Dieser Ausschluss des Rechtsmittels gelte auch für die Pandemie-Sonderregelungen in § 114 III ArbGG und § 211 III SGG. In den Absätzen 1 und 2 dieser Regelungen seien ausdrücklich „von § 128 a ZPO abweichende“ Regelungen für ehrenamtliche Richter (Abs. 1) sowie für die Abstimmung und Entscheidung eines Spruchkörpers (Abs. 2) getroffen. Dagegen regle der jeweilige Absatz 3 lediglich einen Sonderfall des § 128 a I ZPO und schränke das Ermessen des Gerichts dahingehend ein, dass das Gericht den Parteien und ihren Bevollmächtigten bei einer epidemischen Lage von nationaler Tragweite nach § 5 I 1 Infektionsschutzgesetzes „im Falle des § 128 a der Zivilprozessordnung“ von Amts wegen gestatten soll, sich während einer mündlichen Verhandlung an einem anderen Ort aufzuhalten und von dort im Wege der zeitgleichen Bild- und Tonübertragung Verfahrenshandlungen vorzunehmen. Während die Absätze 1 und 2 der Regelungen jeweils „Abweichendes“ zu § 128 a ZPO bzw. § 110 a SGG regelten, fügten sich die jeweiligen Regelungen in Abs. 3 ausdrücklich in die allgemeinen Regelungen von § 128 a ZPO und § 110 a SGG ein. Die allgemeinen Regelungen gälten damit auch für die Pandemie-Sonderregelung in Absatz 3, also insbesondere, dass die Übertragung nicht aufgezeichnet wird (Satz 1) und Entscheidungen über die Gestattung unanfechtbar sind (Satz 2).

In Anbetracht der klaren Regelung in § 128 a III ZPO und § 110 a III SGG hätte zudem ein abweichender Wille des Gesetzgebers im Pandemie-Sondergesetz oder zumindest im Gesetzgebungsverfahren Niederschlag finden müssen.

* Der Autor ist Richter am Landgericht Oldenburg und betreibt einen Blog zum Zivilprozessrecht (<https://www.zpoblog.de/>).

Und eine solche Auslegung sei zuletzt auch deshalb zwingend, weil sonst kein Aufzeichnungsverbot für die Übertragung der Verhandlung zu den Parteien und ihren Bevollmächtigten und Beständen bestünde. In § 114 I 3 ArbGG und § 211 I 3 SGG sei ein solches nur für die Bild- und Tonübertragung zu ehrenamtlichen Richtern statuiert und in den jeweiligen Absätzen 2 für die Beratung und Entscheidung der Spruchkörper. Ein Aufzeichnungsverbot sei indessen auch für die Verhandlung aus datenschutzrechtlichen Gründen unabweisbar geboten.

III. Anmerkung

Die Entscheidung ist – soweit ersichtlich – die erste veröffentlichte obergerichtliche Entscheidung zu den Pandemie-Sonderregelungen in §§ 114 ArbGG und 211 SGG. Mit diesen Regelungen hat der Gesetzgeber im Rahmen des Sozialschutz-Pakets II (BGB I 2020, 1055) zu Beginn der Corona-Pandemie im April 2020 für die Arbeits- und Sozialgerichtsbarkeit Sonderregelungen geschaffen (zu noch weitergehenden Vorschlägen s. z. B. *Oltmanns/Fuhlrott* DB 2020, 841), mit denen aus Gründen des Gesundheitsschutzes die Nutzung von Videokonferenztechnik im Anwendungsbereich des ArbGG und SGG gefördert werden sollte (s. die Begründung des RegE, BT-Drucks. 19/18966, S. 30-32; ausf. *Francken* NZA 2020, 681 (683 f.), sehr kritisch *Greger* MDR 2020, 957 Rn. 22 ff.). Anstelle des lediglich pflichtgemäßen Ermessens in den Regelungen des § 128 a ZPO (i. V. m. § 46 II ArbGG) bzw. § 110 a SGG reduzierte der Gesetzgeber das Ermessen dahin, dass es im Falle einer epidemischen Lage von nationaler Tragweite im Regelfall zu gestatten sei, eine Teilnahme im Wege der Bild- und Tonübertragung zu ermöglichen. Dabei unterlag der Gesetzgeber jedoch wohl einer nicht unerheblichen Fehleinschätzung über den tatsächlichen Zustand der Ausstattung der Arbeits- und Sozialgerichte (S. dazu einerseits den RegE, BT-Drucks. 19/18966, S. 28 und andererseits die Stellungnahme des Bundesrats, BR-Drucks. 245/20 S. 2). Das zeigen nicht zuletzt die hier zu besprechende Entscheidung und die vorangegangene Entscheidung des ArbG Düsseldorf (*ArbG Düsseldorf*, Beschl. v. 25.6.2020 – 9 Ca 3273/20 = BeckRS 2020, 17871). Noch immer verfügen viele Gerichte nicht über die für Verhandlungen im Wege der Bild- und Tonübertragung erforderliche Hard- und Software.

Insoweit erscheint allerdings schon im Ausgangspunkt zweifelhaft, ob das ArbG Düsseldorf in der Ausgangsentscheidung tatsächlich die fehlende Ausstattung im Rahmen der Ermessensausübung berücksichtigen durfte. Denn mit dem Ziel des (Bundes-)Gesetzgebers, die Nutzung von Videokonferenztechnik zu fördern, scheint es kaum zu vereinbaren, könnten die Länder bzw. Gerichtsverwaltungen diese eindeutige gesetzgeberische Wertentscheidung unterlaufen, indem sie die erforderliche Ausstattung unterließen. So ist teilweise die Rede von einem „gegen den Grundsatz der Gewaltenteilung verstoßender Übergriff der Justizverwaltung“,

wenn das Gericht dazu genötigt werde, „zweckwidrige fiskalische Erwägungen des Beschaffungsaufwandes oder gar eine Verweigerungshaltung zu berücksichtigen und so den vom Gesetz verlangten Regelfall zur Ausnahme machen“ (s. *Fichte/Jüttner/Schreiber*, SGG, 3. Aufl. 2020, § 211 Rn. 9). Angesichts der Neuregelung im ArbGG und SGG spricht viel dafür, dass jedenfalls in diesen Gerichtsbarkeiten inzwischen eine Pflicht der Gerichtsverwaltungen besteht, die technischen Voraussetzungen dafür zu schaffen, dem eindeutigen gesetzgeberischen Willen in §§ 114 ArbGG, 211 SGG auch zur Geltung zu verhelfen (ebenso z. B. *Fichte/Jüttner/Schreiber*, SGG, § 211 Rn. 9; für § 128 a ZPO auch BeckOK-ZPO/von Selle, 38. Ed. 09/20, § 128 a Rn. 2.2; *Windau* NJW 2020, 2753 Rn. 19, anders die h. M., s. nur MKLS/B. *Schmidt*, SGG, 13. Aufl. 2020, § 110 a Rn. 3, zu § 128 a ZPO s. auch *Prütting/Gehrlein/Prütting*, ZPO, 12. Aufl. 2020, § 128 a Rn. 1). Besteht eine solche Ausstattungspflicht, kann die tatsächliche Ausstattung für die Ermessensausübung nicht relevant sein (s. ausführlich *Windau* NJW 2020, 2753, Rn. 19; ebenso BeckOK-ZPO/von Selle, § 128 a Rn. 5).

Daneben scheint trotz der sehr sorgfältigen Begründung auch das Ergebnis – die Unanfechtbarkeit zurückweisender Beschlüsse im Anwendungsbereich von §§ 114 III ArbGG, 211 III SGG – nicht zweifelsfrei. Gerade die Umkehrung des Regel-/Ausnahme-Verhältnisses und der erklärte Zweck des Gesetzgebers, die Nutzung von Videokonferenztechnik zu fördern, legen bei der Frage der Anfechtbarkeit eher ein beredtes Schweigen nahe (anders aber z. B. *Schlegel/Voelzke/Herbst*, jurisPK-SGG (Stand: 24.9.2020), § 211, Rn. 36). Und auch das vom LAG Düsseldorf angeführte Argument der fehlenden Verweisung in § 114 III ArbGG auf § 128 a III 1 ZPO und das damit scheinbar fehlende Verbot einer Aufzeichnung überzeugt kaum. Denn einerseits hat der Gesetzgeber dies – nicht aber die (Un-)Anfechtbarkeit – ausdrücklich im Rahmen der Begründung klarstellt (BT-Drucks. 19/18966 S. 30). Und andererseits hat er das Verbot in § 211 III 3 SGG (nicht aber in § 114 III ArbGG) ausdrücklich geregelt. Dass der Gesetzgeber die Frage der Anfechtbarkeit für das ArbGG und das SGG unterschiedlich regeln wollte, wird man kaum annehmen können.

Selbst wenn man aber der Ansicht des LAG folgt, heißt dies nach h. M. allerdings nicht, dass Entscheidungen nach §§ 114 ArbGG, 211 SGG jeder gerichtlichen Kontrolle entzogen wären. Denn sie sind nach der in der Literatur herrschenden Auffassung zusammen mit der Hauptentscheidung anfechtbar, soweit sie sich darauf ausgewirkt hat (s. zu § 128 a ZPO z. B. *MüKoZPO/Fritsche*, 6. Aufl. 2020, § 128 a Rn. 17; *Musielak/Voit/Stadler*, ZPO, 17. Aufl. 2020, § 128 a Rn. 9; zu § 110 a SGG s. MKLS/B. *Schmidt*, § 110 a Rn. 16; anders aber BeckOK-ZPO/von Selle, § 128 a Rn. 15).

Automatisierung von Expertenwissen

In dieser Rubrik werden regelmäßig konkrete Anwendungen vorgestellt, die den beruflichen Alltag vereinfachen, ergänzen oder in sonstiger Weise verbessern können. Dabei handelt es überwiegend um kommerzielle Angebote, die bei Bedarf getestet und am Markt eingekauft werden können. Aber es werden auch sonstige Projekte und Konzepte vorgestellt, um der bestehenden Vielfalt gerecht zu werden. Den Auftakt macht das deutsche Unternehmen Bryter, das mittlerweile auch international von sich reden macht.

Bryter ist sowohl der Name des deutschen Unternehmens mit Sitz in Berlin als auch der Plattform, die angeboten wird. Das Unternehmen wurde von Michael Grupp, Dr. Micha-Manuel Bues und Michael Hübl gegründet.

Welches Problem löst die Plattform?

Im beruflichen Alltag sind viele Tätigkeiten repetitiv. Regelmäßig sind Entscheidungen zu treffen, bei denen immer die gleichen Vorfragen abgearbeitet werden müssen. Oder es sind Dokumente zu erstellen, deren Inhalt sich lediglich in wenigen Variablen unterscheiden, die aber trotzdem jedes Mal manuell und damit zeitaufwendig angepasst werden müssen. Insbesondere wenn nur einzelne Experten für die Entscheidungsfindung oder die Dokumentenerstellung verantwortlich sind, kann dies zu einem Engpass an Kapazitäten und damit zu einer zeitlichen Verzögerung führen. Schließlich besteht die Gefahr, dass unterschiedliche Experten einen unterschiedlichen Entscheidungsweg gehen oder bei der Erstellung von Dokumenten unterschiedliche Bausteine verwenden. Dies kann zu Fehlern führen.

Mit der Bryter-Plattform können diese Prozesse automatisiert und damit vereinheitlicht werden. Im Ergebnis kann mit dieser Plattform jeweils eine Anwendung erstellt werden, die die relevanten Punkte abfragt. Der Experte hat vorher die einzelnen Fragen herausgearbeitet, Antwortmöglichkeiten vorgegeben und die einzelnen Antworten jeweils mit der nächsten Frage verbunden. Das Ergebnis kann dann eine rechtliche Einschätzung oder ein rechtliches Dokument sein. Dieser Ansatz ist seit einiger Zeit beispielsweise für die Erstellung von Steuererklärungen bekannt. Der Vorteil ist nun, dass jeder Experte sein Wissen auf dieser Plattform automatisieren kann – und das völlig ohne Programmierkenntnisse.

Wie funktioniert das?

Die Plattform läuft in der Cloud oder auf dem internen Netzwerk und kann darum von überall über einen Browser ohne vorherige Installation bedient werden. Der Nutzer arbeitet dann auf einer graphischen Oberfläche. Auf dieser Oberfläche werden die einzelnen Entscheidungsknoten mit ein paar Mausklicks erstellt, mit Fragen und Antwortmöglichkeiten befüllt sowie mit den nächsten Fragen verbunden.

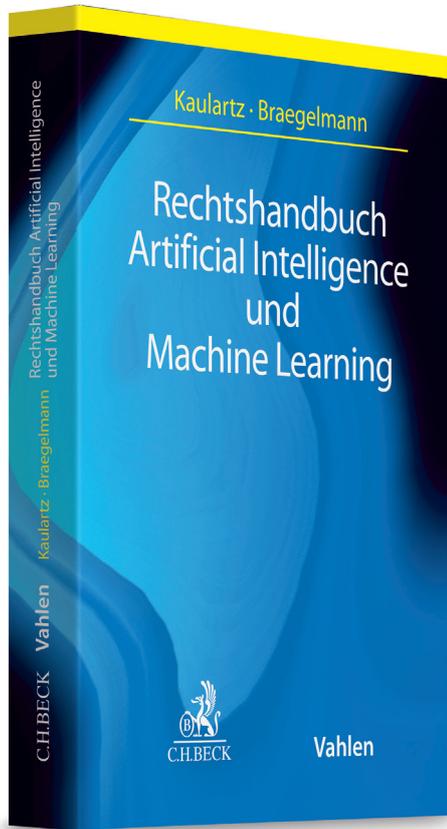
Was kostet das Tool?

Die Plattform wird nach dem typischen Software-as-a-Service Lizenzmodell vertrieben. Die konkrete Preisspanne variiert je nach Anzahl der Nutzer sowie der entwickelten und veröffentlichten Anwendungen.

Eine ähnliche Anwendung

Das aus dem englischsprachigen Raum stammende Unternehmen Neota Logic bietet ebenfalls eine Plattform zur Automatisierung von Expertenwissen an, die sich unter anderem auch speziell an Juristen wendet.

Der Experte für Künstliche Intelligenz und Maschinelles Lernen.



Kaulartz/Braegelmann Rechtshandbuch Artificial Intelligence und Machine Learning

2020. XXXVII, 699 Seiten.
Kartoniert € 169,-
ISBN 978-3-406-74658-1

▶ MIT AUTORENVIDEO ZUM BUCH

☰ beck-shop.de/29876057

VORTEILE AUF EINEN BLICK

- ▶ erläutert technische Hintergründe verständlich
- ▶ übersichtliche Darstellung der praxisrelevanten Rechtsfragen
- ▶ verfasst von Praktikern für Praktiker

Künstliche Intelligenz und Maschinelles Lernen

Die immer weiter fortschreitende Technologie fördert neue und bisher ungekannte Rechtsfragen zutage, auf die es noch keine allgemeingültigen Antworten oder gar Rechtsprechung gibt. Daher widmet sich die Neuerscheinung genau diesen Unbekannten und vermittelt **praktische Lösungsvorschläge** für alle, die im Rahmen der Erstellung und beim Einsatz von Künstlicher Intelligenz beraten.

Das Rechtshandbuch

führt in die unterschiedlichen Ausgestaltungen von **Künstlicher Intelligenz aus technischer Sicht** ein und erörtert im Anschluss verschiedene **praxisrelevante Rechtsfragen**, etwa zu Haftungs-, Vertrags- und Deliktsrecht, Strafrecht, Immaterialgüterrecht, Datenschutzrecht, Gesellschaftsrecht, Verbraucherschutzrecht, Arbeitsrecht, Insolvenzrecht, Streitbeilegungsrecht, Berufsrecht sowie Finanzaufsichtsrecht.

Bestens geeignet

für Anwälte, Unternehmensjuristen, Richter, Referenten/Sachbearbeiter in Behörden sowie Rechtspolitiker.

Erfolgreiche Legal Tech-Strategien entwickeln.



Remmert
**Legal Tech-Strategien
für Rechtsanwälte**
Berufsrecht, Kooperationen, Haftung

2020. XXX, 317 Seiten.

Kartoniert € 89,-

ISBN 978-3-406-74372-6

Neu im November 2020

☰ beck-shop.de/29076167

VORTEILE AUF EINEN BLICK

- behandelt diesen lukrativen Markt für Anwälte
- mit Bezügen zum Datenschutz-, Haftungs-, Versicherungs- und Steuerrecht
- hilft dabei, rechtskonforme Legal Tech-Strategien zu entwickeln

Diese Neuerscheinung

behandelt die berufsrechtlichen Möglichkeiten und Grenzen sowie den **regulatorischen Rahmen** (wie datenschutz-, haftungs-, versicherungs- und steuerrechtliche Fragen) anwaltlicher Legal Tech-Strategien und regt seine Nutzer an, **berufsrechtskonforme Legal Tech-Strategien** zu entwickeln und damit rechtssicher Chancen am lukrativen Markt für **digitale Rechtsdienstleistungen** für sich zu nutzen.

Aus dem Inhalt

- Möglichkeiten und Grenzen nach anwaltlichem Berufsrecht
- Zusammenarbeit mit Legal Tech-Anbietern
- Datenschutzrechtliche Anforderungen
- Haftungs- und versicherungsrechtliche Aspekte
- Sanktionen
- Steuerrechtliche Aspekte
- Ausblick/Reformbedarf

Das perfekte Tool

für Rechtsanwälte und Juristen in Berufsverbänden und -vereinen.



Ihre sichere Quelle für Big Data.

Das Praxishandbuch

Um mit Big Data erfolgreich arbeiten zu können, sind technische Expertise sowie Infrastruktur in Unternehmen eine Grundvoraussetzung. Darüber hinaus sind die **geltenden rechtlichen Spielräume** für die Arbeit mit Big Data unabdingbar. Dies gilt insbesondere im

Hinblick auf die neue **DS-GVO** und die dadurch etablierten Datenschutzanforderungen. Die Neuerscheinung behandelt die damit verbundenen Herausforderungen und hilft dabei, **konkrete Lösungen** zu finden.

Caldarola/Schrey
Big Data und Recht

2019. XX, 184 Seiten.
Kartonierte € 65,-
ISBN 978-3-406-73284-3

≡ beck-shop.de/25836599



Erhältlich im Buchhandel oder bei: beck-shop.de | Verlag C.H. BECK oHG · 80791 München | kundenservice@beck.de | Preise inkl. MwSt. | 169780

facebook.com/verlagCHBECK linkedin.com/company/verlag-c-h-beck twitter.com/CHBECKRecht

ISSN: 2702-2404

RD i Recht Digital

Schriftleitung

Christopher RENNIG (V.i.S.d.P.)
Philipps-Universität Marburg
Universitätsstr. 6, 35037 Marburg
E-Mail: rdi@beck.de

Verlagsredaktion

Dr. Sebastian PECH
Dr. Susanne REINEMANN
Verlag C.H. BECK München/
Frankfurt a.M.

Manuskripte: Manuskripte sind an die Schriftleitung zu senden. Der Verlag haftet nicht für Manuskripte, die unverlangt eingereicht werden. Sie können nur zurückgegeben werden, wenn Rückporto beigelegt ist. Die Annahme zur Veröffentlichung muss schriftlich erfolgen. Mit der Annahme zur Veröffentlichung überträgt der Autor dem Verlag C.H. BECK an seinem Beitrag für die Dauer des gesetzlichen Urheberrechts das exklusive, räumlich und zeitlich unbeschränkte Recht zur Vervielfältigung und Verbreitung in körperlicher Form, das Recht zur öffentlichen Wiedergabe und Zugänglichmachung, das Recht zur Aufnahme in Datenbanken, das Recht zur Speicherung auf elektronischen Datenträgern und das Recht zu deren Verbreitung und Vervielfältigung sowie das Recht

zur sonstigen Verwertung in elektronischer Form. Hierzu zählen auch heute noch nicht bekannte Nutzungsformen. Das in § 38 Abs. 4 UrhG niedergelegte zwingende Zweitverwertungsrecht des Autors nach Ablauf von 12 Monaten nach der Veröffentlichung bleibt hiervon unberührt.

Urheber- und Verlagsrechte: Alle in dieser Zeitschrift veröffentlichten Beiträge sind urheberrechtlich geschützt. Das gilt auch für die veröffentlichten Gerichtsentscheidungen und ihre Leitsätze, denn diese sind geschützt, soweit sie vom Einsender oder von der Schriftleitung erarbeitet oder redigiert worden sind. Der Rechtsschutz gilt auch gegenüber Datenbanken und ähnlichen Einrichtungen. Kein Teil dieser Zeitschrift darf außerhalb der engen Grenzen des Urheberrechtsgesetzes ohne schriftliche Genehmigung des Verlags in irgendeiner Form vervielfältigt, verbreitet oder öffentlich wiedergegeben oder zugänglich gemacht, in Datenbanken aufgenommen, auf elektronischen Datenträgern gespeichert oder in sonstiger Weise elektronisch vervielfältigt, verbreitet oder verwertet werden.

Anzeigenabteilung: Verlag C.H. BECK, Anzeigenabteilung, Wilhelmstraße 9, 80801 München, Postanschrift: Postfach 400340, 80.703 München.

Media-Beratung: Telefon (089) 381 89-687, Telefax (089) 381 89-589.

Disposition, Herstellung Anzeigen, technische Daten: Telefon (089) 381 89-609, Telefax (089) 381 89-589, E-Mail: anzeigen@beck.de
Verantwortlich für den Anzeigenteil: *Bertram Mehling*.

Verlag: Verlag C.H. BECK oHG, Amtsgericht München, HRA 48045, *Besucheradresse:* Wilhelmstraße 9, 80801 München, Postadresse: Postfach 400340, 80703 München, Telefon: (089) 381 89-0, Telefax: (089) 381 89-398, Postbank München IBAN: DE82 7001 0080 0006 2298 02, BIC: PBNKDEFFXXX.

Der Verlag ist oHG. Gesellschafter sind Dr. Hans Dieter Beck und Dr. h.c. Wolfgang Beck, beide Verleger in München.

Bestellungen nehmen jede Buchhandlung und der Verlag entgegen.

KundenServiceCenter:
Telefon: (089) 381 89-750
Telefax: (089) 381 89-358
E-Mail: kundenservice@beck.de

Bezugspreise 2020: Jährlich inkl. RD i Direkt: € 349,- (inkl. MwSt.); Einzelheft: € 32,- (inkl. MwSt.). Versandkosten: jeweils zuzüglich. Die Rechnungsstellung erfolgt zu

Beginn eines Bezugszeitraumes. Nicht eingegangene Exemplare können nur innerhalb von 6 Wochen nach dem Erscheinungstermin reklamiert werden.

Jahrestitellei und -register sind nur noch mit dem jeweiligen Heft lieferbar.

Erscheinungsweise: monatlich.

Abbestellungen müssen 6 Wochen vor Jahresschluss erfolgen.

Adressenänderungen: Teilen Sie uns rechtzeitig Ihre Adressenänderungen mit. Dabei geben Sie bitte neben dem Titel der Zeitschrift die neue und die alte Adresse an.

Hinweis gem. § 7 V der Postdienste-Datenschutzverordnung: Bei Anschriftenänderung des Beziehers kann die Deutsche Post AG dem Verlag die neue Anschrift auch dann mitteilen, wenn kein Nachsendeantrag gestellt ist. Hiergegen kann der Bezieher innerhalb von 14 Tagen nach Erscheinen dieses Heftes beim Verlag widersprechen.

Druck: Mayr Miesbach GmbH, Am Windfeld 15, 83714 Miesbach.



Der Experte für den Elektronischen Rechtsverkehr.



Degen/Emmert
Elektronischer Rechtsverkehr
beA, IT-Sicherheit & Co.

2. Auflage. 2021. XXXV, 271 Seiten mit
zahlreichen Abbildungen.
Kartonierte € 79,-
ISBN 978-3-406-73693-3
Neu im Dezember 2020

☰ beck-shop.de/27223626

VORTEILE AUF EINEN BLICK

- Aktuelles zum besonderen elektronischen Anwaltspostfach (beA)
- enthält Hinweise zum Beweisrecht und zur IT-Sicherheit
- inklusive zahlreicher Schaubilder und Screenshots

Dieses Handbuch

zeigt auf, welche konkreten Änderungen und Investitionen, vor allem auch technischer Art, in Kanzleien, Gerichten, Behörden und Unternehmen in den nächsten Jahren aufgrund der **Neuregelungen zum elektronischen Rechtsverkehr** vorzunehmen sind und erleichtert den Beteiligten somit die erforderliche Umstellung.

Behandelt werden dabei die Themen: ▸ Besonderes elektronisches Anwaltspostfach (beA) ▸ Beweisrecht ▸ IT-Sicherheit ▸ Ersetzendes Scannen ▸ Digitale Langzeitarchivierung ▸ Sicherer Versand mit DE-Mail ▸ Best Practice.

Die Neuauflage 2020

Aktuell eingearbeitet sind insbesondere die ersten Erfahrungen mit dem empfangsfähigen besonderen elektronischen Anwaltspostfach (beA). Die Neuauflage berücksichtigt zudem alle weiteren **Entwicklungen beim elektronischen Rechtsverkehr**, wie die technischen Fortschritte bei der e-Justiz, dem e-Government und den Archivierungsdiensten für Anwälte und Gerichte.

”

Den Autoren gelingt es, die ineinander greifenden Fragen von Recht und Technik anschaulich zu erläutern, nicht zuletzt auch mit Hilfe von Checklisten, Grafiken und Screenshots.

Prof. Dr. Matthias Kilian, in: AnwBl 02/2017, zur Voraufgabe

Geschäftsführende Herausgeber

Prof. Dr. Florian Möslein, Dipl.-Kfm., LL.M. (London), Inhaber des Lehrstuhls für Bürgerliches Recht, Deutsches und Europäisches Wirtschaftsrecht an der Philipps-Universität Marburg und Gründungsdirektor des Instituts für das Recht der Digitalisierung (IRDi)

Prof. Dr. Thomas Riehm, Inhaber des Lehrstuhls für Deutsches und Europäisches Privatrecht, Zivilverfahrensrecht und Rechtstheorie und Sprecher des Instituts für das Recht der Digitalen Gesellschaft (IRDG) der Universität Passau

Dr. Markus Kaulartz, Rechtsanwalt, CMS Hasche Sigle, München

Herausgeberinnen und Herausgeber

Tom H. Braegelmann, LL.M. (Cardozo), Rechtsanwalt, Attorney and Counsellor at Law (New York), BBL Bernsau Brockdorff & Partner, München

Dr. Julia von Buttler, LL.M. (Duke), Regierun-
gsdirektorin, Bundesanstalt für Finanzdienstleistungs-
aufsicht (BaFin), Frankfurt a.M.

Prof. Dr. Martin Ebers, Professor für IT-Recht Universität Tartu (Estland), Privatdozent an der Juristischen Fakultät der Humboldt-Universität zu Berlin sowie Präsident der Rechtswissenschaftlichen Gesellschaft für Künstliche Intelligenz und Robotik – Robotics & AI Law Society e.V. (RAILS)

Dr. Tobias Faber, Rechtsanwalt und Partner, Hogan Lovells International LLP, Frankfurt a.M.

Dr. Martin Fries, LL.M. (Stanford), Privatdozent an der Juristischen Fakultät der Ludwig-Maximilians-Universität, München

Dr. Dennis-Kenji Kipker, Geschäftsführer Certavo GmbH, Wissenschaftlicher Geschäftsführer des Instituts für Informations-, Gesundheits- und Medizinrecht (IGMR), Universität Bremen und Legal Advisor, Verband der Elektrotechnik, Elektronik und Informationstechnik (VDE), Frankfurt a.M.

Nico Kuhlmann, Rechtsanwalt, Hogan Lovells, International LLP, Hamburg

Dr. Christina-Maria Leeb, Wissenschaftliche Mitarbeiterin und Analyst Digital Business Development, Heussen Rechtsanwalts-gesellschaft mbH, München

Prof. Dr. Kai von Lewinski, Inhaber des Lehrstuhls für Öffentliches Recht, Medien- und Informationsrecht, Universität Passau

Robin Matzke, Rechtsanwalt, Berlin

Dr. Henning Müller, Direktor des Sozialgerichts Darmstadt und Lehrbeauftragter der Philipps-Universität Marburg

Prof. Dr. Sebastian Omlor, LL.M. (NYU), LL.M. Eur., Inhaber der Professur für Bürgerliches Recht, Handels- und Wirtschaftsrecht, Bankrecht sowie Rechtsvergleichung, Philipps-Universität Marburg, Gründungsdirektor des Instituts für das Recht der Digitalisierung (IRDi)

Dr. Gerald Reger, Rechtsanwalt und Fachanwalt für Steuerrecht, Partner, Leiter des Fachbereichs Corporate und der Practice Group Capital Markets, Noerr LLP, München

Dr. Frank Remmert, Rechtsanwalt und Fachanwalt für IT-Recht sowie für gewerblichen Rechtsschutz, Remmert Legal, München

Dr. Thomas Sassenberg, LL.M., Rechtsanwalt, Fachanwalt für Medien- und Urheberrecht, Frankfurt a.M.

Prof. Dr. Martin Schmidt-Kessel, Inhaber des Lehrstuhls für Deutsches und Europäisches Verbraucherrecht und Privatrecht sowie Rechtsvergleichung, Universität Bayreuth

Dr. Lea Maria Siering, Rechtsanwältin, Finleap, Berlin

Dr. Alexander Steinbrecher, LL.M. (Tulane), Rechtsanwalt, Head of Group Corporate, M&A and Legal Affairs, Bombardier Transportation, Berlin

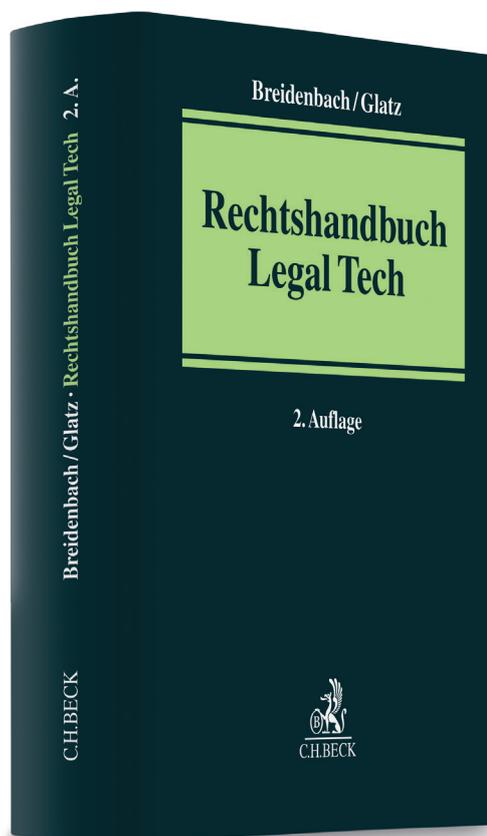
Prof. Dr. Björn Steinrötter, Inhaber der Juniorprofessur für IT-Recht und Medienrecht (Tenure Track), Universität Potsdam

Rebekka Weiß, LL.M. (Glasgow), Leiterin Vertrauen & Sicherheit, Bitkom e.V., Berlin

Benedikt Windau, Richter am LG Oldenburg, Gründer und Herausgeber von zpoblog.de

Prof. Dr. Thomas Wischmeyer, Inhaber des Lehrstuhls für Öffentliches Recht und Recht der Digitalisierung, Universität Bielefeld

Legal Tech – die Zukunft der Rechtsberatung.



Breidenbach/Glatz Rechtshandbuch Legal Tech

2. Auflage. 2021. Rund 420 Seiten.

In Leinen ca. € 129,-

ISBN 978-3-406-73830-2

Neu im Januar 2021

☰ beck-shop.de/27489151

VORTEILE AUF EINEN BLICK

- übersichtliche Darstellung der Veränderungen im Rechtsmarkt
- zahlreiche Anwendungsbeispiele aus der Praxis
- Trendanalyse für die kommenden 10–15 Jahre

Das aktuelle Rechtshandbuch

beschreibt anschaulich die Folgen der Digitalisierung des Rechts für die juristischen Berufe, Unternehmen und Verbraucher. Es erläutert die aktuellen Anwendungsfelder von Legal Tech und deren Vorteile für das Angebot und die Nachfrage von Rechtsdienstleistungen.

Aktuelle Trends

Das Handbuch behandelt insbesondere die drei Bereiche:

- Industrialisierung des Rechts (Standardisierung)
- Künstliche Intelligenz (Machine Learning) und
- Vernetzung (Blockchain).

Von führenden Experten

Dargestellt wird die dynamische Materie von führenden Protagonisten der Legal-Tech-Szene im In- und Ausland. Zahlreiche Anwendungsbeispiele verdeutlichen die Aktualität der durch Legal Tech verursachten Veränderungen im Rechtsmarkt.



Ein spannendes Werk, das den Horizont öffnet ...

Dr. Philipp Kramer, in: www.datenschutz-berater.de 05/2018, zur Voraufgabe

Der richtige Umgang mit Künstlicher Intelligenz und Robotik.

Das neue Handbuch

bietet eine **praxisbezogene** und zugleich **wissenschaftlich fundierte Darstellung** der Rechtsfragen der KI und smarten Robotik. Es gibt als erstes Werk einen **juristischen Gesamtüberblick** hinsichtlich dieser sich dynamisch entwickelnden und zunehmend in den Fokus von Wirtschaft, Wissenschaft, Politik und breiter Öffentlichkeit rückenden Technologien.

Aus dem Inhalt

- Technische Grundlagen der KI und der Robotik
- Regulierung
- Vertragsrechtliche Fragestellungen
- Zivilrechtliche Haftung für KI und smarte Robotik
- Verbraucherrecht
- Strafrechtliche Implikationen von KI und Robotik
- Arbeitsrechtliche Probleme von KI und Robotik
- KI im Urheber- und im Patentrecht
- KI-spezifische datenschutzrechtliche Herausforderungen
- KI-spezifische Rechtsfragen der Cyber-Sicherheit
- KI im Gesellschaftsrecht
- Kapitalmarkt- und Finanzdienstleistungsrecht
- Versicherungsrecht
- Wettbewerbsrecht
- Telekommunikationsrecht
- KI im Prozessrecht
- Regierungs- und Verwaltungshandeln durch KI
- KI und Steuerrecht

Die Neuerscheinung

enthält zahlreiche Anwendungsbeispiele, etwa zu Legal Tech, automatisiertem Transport, Industrie, Smart Devices & Wearables, Personal Robots, Smart Contracts und Blockchain, Medizin, Plattformen und KI, Verbrechensbekämpfung. So lässt sich das theoretische Know-how in der Praxis leichter umsetzen.



Ebers/Heinze/Krügel/Steinrötter
Künstliche Intelligenz und Robotik

2020. LI, 1034 Seiten.
In Leinen € 199,-
ISBN 978-3-406-74897-4
Neu im Oktober 2020

☰ beck-shop.de/30097161